现代应用数学丛书

# 试验设计法

〔日〕增山元三郎 著

上海科学技术出版社

现代应用数学丛书

# 試驗設計法

——設計的理論——

〔日〕增山元三郎 著
刘 璋 温 譯

上海科学技术出版社

## 內容提要

本书是日本岩波书店出版的現代应用数学丛书之一的中譯本，敘述試驗設計的数学理論。全书共四章和一个附录。第1章說明 BIB 設計的优点，第2章詳細討論如何用有限射影几何來構造 BIB 設計，第3章扼要介紹因子試驗，包含正交陣列的构造，第4章討論設計的存在条件。附录簡短地敘述构造上述設計用到的 Galois 域的知識。书末还附有 BIB 設計表(附表1)和最小函数表(附表2)。另外，为了便于讀者查閱，譯者补充了本书引用到的和本书原书出版后的一些新文献。本书可供高等学校概率統計专业的师生以及試驗設計工作者、研究人員参考。


現代应用数学丛书

**試驗設計法**(設計的理論)

原 书 名 実験計画法—配置の型の理論
原 著 者 〔日〕增 山 元 三 郎
原出版者 岩 波 书 店，1957
譯 者 刘 璋 温

*

上海科学技术出版社出版
(上海瑞金二路150号)
上海市书刊出版业营业許可証出093号
新华书店上海发行所发行 各地新华书店經售
商务印书館上海厂印刷

*

开本 850×1168 1/32 印張 3 22/32 字数 85,000
1963年3月第1版 1963年3月第1次印刷
印数 1—4,000

統一书号：13119・496
定 价：(十四) 0.64元

# 出版説明

这一套书是根据日本岩波书店出版的"現代应用数学讲座"翻譯而成。日文原书共15卷60册，分成A、B两組，各編有序号。現在把原来同一題目分成两册或三册的加以合并，整理成42种，不另分組編号，陆續翻譯出版。

这套书涉及的面很广，其內容都和現代科学技术密切有关，有一定参考价值。每一本书收集的資料都比較丰富，而叙述扼要，篇幅不多，有利于讀者以較短时間掌握有关学科的主要內容。虽然，这套书的某些观点不尽适合于我国的情况，但其方法可供参考。因此，翻譯出版这一套书，对我国学术界是有所助益的。

由于日文原书是1957年起以讲座形式陆續出版的，写作时間和篇幅的限制不可避免地会影响原作者对內容的处理，为了尽可能地減少这种影响，我們在每一譯本中，特請譯者或校閱者撰写序或后記，以介紹有关学科的最近发展状况，并对全书內容作一些評价，提出一些看法，結合我国情况补充一些資料文献，在文內过于簡略或不足的地方添加了必要的注釋和改正原书中存在的一些錯誤。希望这些工作能对讀者有所帮助。

承担翻譯和校閱的同志，为提高书籍的质量付出了巨大劳动，在此特致以誠摯的謝意。

欢迎讀者对本书提出批評和意見。

上海科学技术出版社

# 現代应用数学丛书

| 书名 | 原作者 | 譯者 | 书名 | 原作者 | 譯者 |
|---|---|---|---|---|---|
| 代数学* | 弥永昌吉等 | 熊全淹 | 非綫性振动論* | 古屋茂 | 呂紹明 |
| 几何学* | 矢野健太郎 | 孙澤瀛 | 力学系与映射理論* | 岩田义一 | 孙澤瀛 |
| 复变函数 | 功力金二郎 | 刘书琴 | 平面彈性論* | 森口繁一 | 刘亦珩 |
| 集合·拓扑·测度* | 河田敬义 | 賴英华 | 有限变位彈性論 变形几何学* | 山本善之 近藤一夫 | 刘亦珩 |
| 泛函分析* | 吉田耕作 | 程其襄 | 塑性論* | 鷲津久一郎 | 刘亦珩 |
| 广义函数* | 岩村联 | 楊永芳 | 粘性流体理論* | 谷一郎 | 刘亦珩 |
| 常微分方程* | 福原滿洲雄 | 張庆芳 | 可压縮流体理論* | 河村龙馬 | 刘亦珩 |
| 偏微分方程* | 南云道夫 | 錢端壮 | 网絡理論 | 喜安善市等 | 賈弃馨 |
| 特殊函数* | 小谷正雄等 | 錢端壮 | 自动控制理論* | 喜安善市等 | 翟立林 |
| 差分方程* | 福田武雄 | 穆鴻基 | 回路拓扑学 | 近藤一夫 | 張鳴鏞 |
| 富里哀变换与拉普拉斯变换* | 河田龙夫 | 錢端壮 | 信息論* | 喜安善市等 | 李文清 |
| 变分法及其应用* | 加藤敏夫 | 周怀生 | 推断統計理論 | 北川敏男 | 李賢平 |
| 李群論* | 岩堀长庆 | 孙澤瀛 | 統計分析* | 森口繁一 | 刘璋温 |
| 随机过程* | 伊藤清 | 刘璋温 | 試驗設計法 | 增山元三郎 | 刘璋温 |
| 回轉群与对称群的应用* | 山内恭彦等 | 張质賢 | 群体遺傳学的数学理論* | 木村資生 | 刘祖洞 |
| 結晶統計与代数* | 伏見康治 | 孙澤瀛 | 博奕論 | 宫澤光一 | 張毓春 |
| 偏微分方程的应用 | 犬井鉄郎等 | 楊永芳 | 綫性規划 | 森口繁一 | 刘源張 |
| 微分方程的近似解法 | 加藤敏夫等 | 王占瀛 | 經济理論中的数学方法 | 安井琢磨等 | 談祥柏 |
| 数值計算法 | 森口繁一等 | 閻昌齡 | 随机过程的应用* | 河田龙夫 | 刘璋温 |
| 量子力学中的数学方法* | 朝永振一郎 | 周民強 | 計算技术 | 高桥秀俊 | 姚晋 |
| 工程力学系統* | 近藤一夫等 | 刘亦珩 | 穿孔卡計算机 | 森口繁一 | 刘源張 |

注：有*者已在1962年出版。

# 譯者序

試驗設計法是数理統計学中的一个重要分支，它是在近四十年来，由于农业和工业的需要，以及由于它本身內在的数学問題的解决而迅速发展起来的一門学科。

試驗設計首先由英国統計学家 R. A Fisher 在他的經典著作 The Design of Experiments (1926) 中引进。Fisher 在該书中提出了两个設計，一个叫做随机区組(完全区組)，另一个叫做拉丁方，它們分別是現在称为多种方式分組設計和部分実施法的特殊情形。1936 年，Fisher 的学生 F. Yates 把完全区組設計推广为不完全区組設計。随后，有不少数学家，特别是印度学派，对构造不完全区組和拉丁方的数学理論作出了有价值的貢献。本书主要介紹不完全区組中的平衡不完全区組設計。

不完全区組設計包含着很多数学問題，因而在它一出現之后就引起了广大統計学家和部分数学家的注意。1959 年，通过平衡不完全区組設計的研究，印度学者 R. C. Bose 和 S. S. Shrikhande 以及美国学者 E. T. Parker 等人，打破了將近二百年来一直被认为是眞实的 Euler 关于不存在 $4t+2$ 阶正交拉丁方的猜想。在他們已得結果的推动下，正交拉丁方的研究比从前更加活跃了。

当然，人們对研究試驗設計感到兴趣，不只是因为它包含許多数学問題。試驗設計，从其名称可以看出，是一門应用性較强的学科，它的应用范圍几乎已扩及到自然科学和社会科学的大部分研究領域。

近年来，国外用各种文字出版的試驗設計法的书已为数不少，

但在我国,这样一本书的出版还可算是第一次❶。譯者希望,本书的出版能使更多的讀者了解数学在試驗設計法中所起的作用,并引起更大的兴趣。

在翻譯过程中,为了使原书的意义更清楚,作了一些必要的注解,并补充了若干书中引到的以及原书出版以后发表的文献,希望能对讀者有所助益。但因限于水平,挂一漏万,錯誤在所难免,請給予批評指正。

刘 璋 温

1962年10月,北京

---

❶ K. A. 勃郎里著(陈蔭枋譯),工业試驗統計(科学出版社,1959)一书只讲实际应用,而不讲設計的数学理論。

# 序

本书所介紹的是試驗設計法中用到的各种設計的理論，而不是利用这些設計来做試驗，然后讲述对試驗結果进行統計分析的方法❶。設計的理論迄今仍未充分齐整，大致已属完整的，可以举出多种方式分組設計中的固定模型的情形。这可在 A. Wald 的讲义[10]或者 H. B. Mann 的书[6]中找到❷。这里我們愿意把理論尚未完整的設計提出来，着重介紹用什么方法已解决到什么地步。但是由于篇幅的限制，对于看来希望不大的方法，不能不割爱了。

在第 1 章中，我們提出了最不完整而且不具有正交性的設計，亦即不完全区組設計，并且給出了它的定义和存在的問題。在第 2 章中，我們主要地討論了把满足給定試驗条件的解变为几何問題来求，这相当于解存在的充分条件。在第 3 章中，我們介紹了正交設計的几种构造方法，而其中水平数不相同的正交陣列的一般理論和强度不一样的正交陣列的一般理論，仍未解决❸。在最后一章，即第 4 章中，我們介紹了平衡不完全区組設計存在的必要条件，但这与上述的充分条件尚有相当大的距离。根据我們在§2中的研究結果，如果不按照参数的数論性质把設計更加細分，并个别地求其存在条件，那末这个距离看来不能縮小。

附表 1 列举了，当把試驗分为 $b$ 个区組进行时，在 $b \leqslant 100$ 的

---

❶ 見本丛书森口繁一：統計分析，刘璋温譯，1962.

❷ 著者已把这两本书的概要介紹于中山伊知郎編：統計学辞典，东洋經济出版社，东京，1951，增补版，1957.

❸ 見增山元三郎：穿孔カードによる実験の計画とその解析，日本科学技术連盟，东京，1957，§23.

范圍內迄今已知的平衡不完全区組設計。把依 R. C. Bose 的意义不是同构而是广义同构的設計区别开来，这在实用上并没有很大的意义，所以对于同一参数的設計，表中仅列出了表現簡单的那一个。同样，由单純的重复来增加区組个数而产生的設計，也不列出。但是这个表比現有的任何一个表❶❷都为丰富。

从介紹設計的理論这个意义来說，缺少部分平衡不完全区組(PBIB: partially balanced incomplete block) 的理論，是不妥当的。但是，这种設計計算麻煩而且不太实用，而稍有实用的情形已被印成一本书❸❹，其中包含了表和理論。

起初，为使讀者不一定要参考原論文或者其他参考书也能看懂，著者在編写时把有关的証明都詳細写出，以致篇幅过大。后来作了修改，假定讀者具有相当于岩波全书《实驗計画法》(即[8])程度的知識，尽量把詳細的証明和其他书中已有的証明删去。虽然如此，著者仍然相信，修改后的本书还是能实現著者最初的目的，

---

❶ 例如北川敏男・三留三千男：实驗計画要因配置表，培風館，东京，1953.

❷ Fisher-Yates [28] 和 W. G. Cochran and G. M. Cox: Experimental Designs, 2nd ed., John Wiley & Sons, New York, 1957, 都有詳尽的表。但是，到此为止，所有这些表都是对 $r \leqslant 10$ 造出的，而本书附表 1 中却有几个 $r>10$. 最近 Rao [48] 对 $11 \leqslant r \leqslant 15$ 的 $r$ 做了研究。——譯者注

❸ R. C. Bose, W. H. Clatworthy and S. S. Shrikhande: Tables of Partially Balanced Designs with Two Associate Classes, *Univ. North Carolina, Mimeo. Ser.*, **77**, 1953.

❹ 脚注❸的表在国內可能不容易找到。关于 PBIB 設計，可参看下列文献：

1) R. C. Bose and W. S. Connor: Combinatorial properties of group divisible incomplete block designs, *Ann. Math. Stat.*, **23** (1952), 367～383.

2) R. C. Bose and K. R. Nair: Partially balanced incomplete block designs, *Sankhyā*, 4 (1939), 337～372.

3) R. C. Bose and T. Shimamoto: Classification and analysis of partially balanced incomplete block designs with two associate classes, *J. Amer. Stat. Assn.*, **47** (1952), 151～184.

其中 3) 是首創著作。——譯者注

即介紹'問題的所在,解決問題的方法以及其界限'。

試驗設計的模型,除了本书列举的以外,还可无穷地創造出来。因此,設計的理論尚有推广的余地。迄今已得結果的介紹,若能成为新的推广的出发点,著者将感到无任荣幸。

# 目　录

# 第1章　不完全区組設計

## §1 不完全区組設計

設对 $v$ 个品种 $V_i$ $(i=1, 2, \cdots, v)$ 的每亩收成，用 $b$ 块田 $B_j$ $(j=1, 2, \cdots, b)$ 做試驗进行比較。我們規定，当品种 $V_i$ 被包含于区組(田) $B_j$ 时，$n_{ij}=1$，其他情形时，$n_{ij}=0$。矩陣 $\boldsymbol{A}=(n_{ij})$ 叫做**結合矩陣**❶。这个矩陣的第 $i$ 行元素的和 $r_i$ 表示品种 $V_i$ 被包含于多少个区組，叫做 $V_i$ 的**实施数**❷；第 $j$ 列元素的和 $k_j$ 表示区組 $B_j$ 包含多少个品种，叫做区組 $B_j$ 的**大小**。

$$r_1+r_2+\cdots+r_v=k_1+k_2+\cdots+k_b \stackrel{\mathrm{d}}{=} N \tag{1.1}$$

**是試驗总数**。式中等号上的 d 表示定义式。如果 $B_j$ 的大小不依赖于 $j$ 而等于 $v$，那末这种設計叫做**完全区組設計**(R. A. Fisher, 1926)❸。若把一块田的大小取得过大，則土地肥沃度的不匀性产生影响，以致当把品种位置的排列随机化时，外表上的誤差有趋大的傾向。为了避免这一点，如果取每一区組大小都小于 $v$，那末这种設計叫做**不完全区組設計**(F. Yates, 1936)❹。

$$\lambda_{ij} \stackrel{\mathrm{d}}{=} \sum_{l=1}^{b} n_{il}n_{jl} \quad (i \neq j) \tag{1.2}$$

是两个不同品种 $V_i$ 与 $V_j$ 被包含于同一区組的次数，叫做两者**相遇数**。特别，当 $i=j$ 时，定义

$$\lambda_{ii} \stackrel{\mathrm{d}}{=} r_i. \tag{1.3}$$

---

❶ 也称关联矩陣(incidence matrix)。——譯者注

❷ 也称重复数(number of replication)。——譯者注

❸ Fisher[26]。——譯者注

❹ Yates[65]。——譯者注

在不完全区組設計中，特别若实施数，区組大小以及相遇数都不依賴于足碼而为一定，即分别等于 $r$, $k$, $\lambda$, 則叫做**平衡不完全区組**(**BIB**: balanced incomplete block)。又若

$$v=b, \qquad (1.4)$$

則叫做**对称平衡不完全区組** (**SBIB**: symmetrical balanced incomplete block)。在 BIB 中，試驗总数是

$$N=vr=bk. \qquad (1.5)$$

考虑特定一个品种，譬如 $V_1$ 的比較对手，允許重复，就总共有 $M$ 品种，

$$M\stackrel{d}{=}\lambda(v-1)=r(k-1) \text{❶}. \qquad (1.6)$$

(1.5) 和 (1.6) 是 BIB 存在的必要条件，但不是充分条件❷。如附表 1 中用十字架所示那样，有些 $v$, $k$, $b$ 的組合虽然滿足这两个条件，但 BIB 却不存在。$v$, $k$, $b$, $r$ 和 $\lambda$ 叫做 BIB 的**第一类参数**。

与 $V$ 对偶地考虑 $B$. 一般，令 $\mu_{gh}$ 表示不同区組 $B_g$ 和 $B_h$ 所包含的公共品种的个数，这叫做两区組的**公有数**，

$$\mu_{gh}\stackrel{d}{=}\sum_{i=1}^{v} n_{ig}n_{ih}. \qquad (1.7)$$

特別，当 $g=h$ 时，定义

$$\mu_{gg}\stackrel{d}{=}k_g. \qquad (1.8)$$

在 BIB 中，固定一个区組，譬如 $B_1$，找出与 $B_1$ 公有数为 0 的

---

❶ 关系式(1.6)是这样得到的：一方面，特定一个品种 $V_1$ 出現 $r$ 次，每次同它直接比較的品种有 $(k-1)$ 个，所以总共有 $r(k-1)$ 个；另一方面，$V_1$ 以外的 $(v-1)$ 个品种分别同 $V_1$ 直接比較 $\lambda$ 次，所以总共有 $\lambda(v-1)$ 个。$r(k-1)$ 与 $\lambda(v-1)$ 应該相等。——譯者注

❷ 对于 $k=3$ 以及 $\lambda=1$ 或者 2，条件是充分的，見 Bose[15]. 最近 Hanani[33] 証明了：对 $k=3, 4$ (和所有的 $\lambda$) 以及 $k=5$, $\lambda=1, 4, 20$, 条件也是充分的，但有可能的例外情形：$k=5$, $\lambda=1$, $v=141$.——譯者注

区組，为 1 的区組，等等，再就其頻数分布求方差，这决不为負。由此推出 **R. A. Fisher 不等式**[1]

$$b \geqslant v. \tag{1.9}$$

在 BIB 中，特别当区組个数 $b$ 为 $r$ 的倍数，即

$$b = nr \tag{1.10}$$

的情形，如果能适当地把区組全体分为各有 $n$ 个区組的 $r$ 組，使得每一品种在每一組中只出現一次，那末这种設計叫做**可分解平衡不完全区組**（**RBIB**: resolvable balanced incomplete block）(R. C. Bose, 1942)[2]。参看 §10 的例 1。在 RBIB 中，从 (1.5) 推出 $v=nk$. RBIB 的統計分析跟 BIB 相同，但也可当作多因子試驗的特殊情形来分析。比較这两种情形，便可以知道，为了除掉土地肥沃度的不匀性而縮小区組大小是否有效。在 RBIB 中，令 $B_{\alpha\beta}$ 表示第 $\alpha$ 組的第 $\beta$ 个区組。固定 $B_{01}$，令 $l_{\alpha\beta}$ 表示 $B_{\alpha\beta}(\alpha\neq 0)$ 与 $B_{01}$ 的公有数。对 $l_{\alpha\beta}$ 采用与 (1.7) ~ (1.9) 相同的方法，便可推出 **R. C. Bose 不等式**[3]

$$b \geqslant v+r-1. \tag{1.11}$$

特别当等号成立时，亦即 $l_{\alpha\beta}$ 的方差为 0 的情形，

$$b = v+r-1. \tag{1.12}$$

这种情形叫做**仿射可分解平衡不完全区組**（**ARBIB**: affine resolvable balanced incomplete block）(R. C. Bose, 1942)。在 ARBIB 中，$B_{01}$ 与 $B_{\alpha\beta}(\alpha\neq 0)$ 的公有数为一定，并且

---

[1] Fisher 的原証明，見 Fisher[27] 或者 H. B. Mann [6]，128～129. 另一个証明，見 Bose [18].——譯者注

[2] Bose [16].——譯者注

[3] 由可分解性推出 $v=nk$，但逆不一定成立。Roy [49]，Mikhail [40] 和 Marty [41] 不假定可分解性而在較弱的假定 $v=nk$ 下也分别証明了这个不等式。——譯者注

$$k^2/v=k/n\overset{d}{=}c \tag{1.13}$$

也为一定且是整数。这时

$$r=(cn^2-1)/(n-1), \tag{1.14}$$

且在

$$\lambda=(cn-1)/(n-1)=c+(c-1)/(n-1)\overset{d}{=}c+t \tag{1.15}$$

中 $t$ 是0或者正整数。利用 $t$ 和 $n$ 为補助参数,就在 ARBIB 中,

$$\left.\begin{array}{l} v=n^2[1+(n-1)t],\ k=n[1+(n-1)t], \\ b=n[1+n(1+nt)], \\ r=1+n(1+nt),\quad \lambda=nt+1, \\ E=n(nt+1)/[1+n(1+nt)], \end{array}\right\} \tag{1.16}$$

此处 $E$ 是下节叙述的效率因子。特别,令

$$t\overset{d}{=}(n^N-1)/(n-1),\quad n\overset{d}{=}p^s, \tag{1.17}$$

此处 $p$ 是素数,$s$ 是正整数,则这种情形与由§9中的仿射几何 $EG[N+2,p^s]$ 所构造的設計一致。从(1.16)显然看出,在ARBIB中

$$\lambda+k=r. \tag{1.18}$$

对一个 BIB,(i)更換品种号碼,或者(ii)更換区組号碼后,仍是一个 BIB. 依 R. C. Bose 意义,称如此得到的 BIB 与原来的 BIB **同构**。品种在区組内的順序虽不被指定,但对 SBIB 的情形,利用 Dénes König (1914) 的**分綫色定理**❶,給予 $v$ 个白球(品种)和 $b$ 个黑球(区組),用 $k$ 种色綫联系它們表示結合关系,就可以作出 $k$ 行 $b$ 列的品种排列,使得一列表示一区組内的品种,并且每一品种在每一行只出現一次。亦即把被同一色綫联系的球放在同一行。参看例1的图1.1。这种排列是**不完全拉丁方** (F. Yates, 1936) ❷ 的

❶ Dénes König: Theorie der endlichen und unendlichen Graphen (Akad. Verlag, Berlin, 1936) (Chelsea 版, 1950).

❷ Yates [66].——譯者注

特殊情形，而不完全拉丁方是从边长为 $v$ 的拉丁方 (§ 14) 中留下适当的 $k$ 行并去掉其余的行后得到的，这也叫做 **Youden 方** (W. J. Youden, 1937) ❶。現在所知道的 Youden 方，都是由一行的循环置換得到其他行的，但在 § 14 中叙述的拉丁方則不完全如此。在拉丁方中，有些通过行与行，列与列以及字母与字母的交換也不能从一个变換到另一个。但是，其中有些通过証明分綫色定理时用到的綫色的交換，也可以从一个变換到另一个。把依 Bose 意义虽不同构但是如此广义同构的 BIB 区别开来，不管数学上的意义怎么样，在实用上并沒有很大价值。在这个意义下，即使由循环置換得不到的 BIB 存在，但当令第一类参数相等，并由循环置換可以得到与此广义同构的 BIB，那末尽量研究由循环置換得到的解，就也充分地满足实用上的需要。但其实也存在着 § 15 將叙述到的那种例子。必須留意，由循环置換得到的解，可用穿孔卡机器或者电子計算机按辞典方式求出。附表 1 列出了 $b \leqslant 100$, $k \leqslant 30$ 的范圍內的 BIB.

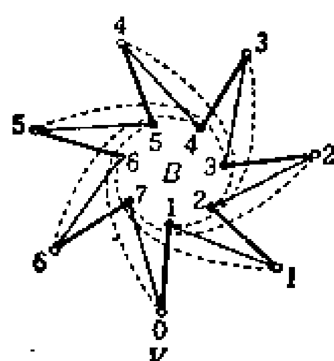


图 1.1

表 1.1

| | $B_1$ | $B_2$ | $B_3$ | $B_4$ | $B_5$ | $B_6$ | $B_7$ |
|---|---|---|---|---|---|---|---|
| $E$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| $P$ | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| $P^3$ | 3 | 4 | 5 | 6 | 0 | 1 | 2 |

**例 1** $v=b=7$, $k=r=3$, $\lambda=1$ 的 SBIB. 先在第一个区組中給予品种号碼，然后作循环置換便得到。例如 (0, 1, 3), (1, 2, 4), …. 第一个区組叫做**初始区組**。关于循环的几何意义，可参看图 8.1。

表中的 $P$ 表示从第一行移到第二行的字母的置換，$E$ 表示恒等置換，

❶ Youden [67].——譯者注

$P^7=E$. 这个初始区組包含的数字有这样的特性:以 $v=7$ 为模考虑所有可能的差,則除 0 以外,从 1 到 $v-1$ 各出現 $\lambda=1$ 次。关于这个差,可参看 §11。

## §2 构造模型与設計的优点❶

把区組 $B_j$ 内的品种 $V_i$ 的收成看做随机变数 $Y_{ij}$ 的实現值,并設它的构造模型为

$$Y_{ij}=\alpha_i+\beta_j+Z_{ij}, \quad \left.\begin{array}{l} i=1, 2, \cdots, v, \\ j=1, 2, \cdots, b. \end{array}\right\} \tag{2.1}$$

此处 $\alpha_i$ 表示因子 $V_i$ 的效应,$\beta_j$ 表示因子 $B_j$ 的效应。这个綫性模型,如果依品种产生的收成差异以及依区組产生的收成差异太小,那末可以认为它很好地反映了实际情况。試驗的目的是,去掉試驗場所的影响 $\beta_j$,以便檢驗未知参数 $\alpha_1, \alpha_2, \cdots, \alpha_v$ 之間有否差异,如果有差异,則去估計这个差异。一般的綫性构造模型由

$$Y_i=\beta_1 g_{1i}+\beta_2 g_{2i}+\cdots+\beta_p g_{pi}+Z_i, \quad i=1, 2, \cdots, N \tag{2.2}$$

給出,此处 $\beta_\alpha (\alpha=1, 2, \cdots, p)$ 是未知参数,$g_{\alpha i}$ 是由試驗設計或者輔助测定而定的已知常数。我們把 $Y_i$, $y_{\alpha i}$ 和 $Z_i$ 分别看做 $N$ 維 Euclid 空間的矢量 $\boldsymbol{Y}$, $\boldsymbol{g}_\alpha$ 和 $\boldsymbol{Z}$ 的第 $i$ 个正交分量,并記

$$\boldsymbol{Y}=\beta_1\boldsymbol{g}_1+\beta_2\boldsymbol{g}_2+\cdots+\beta_p\boldsymbol{g}_p+\boldsymbol{Z}. \tag{2.3}$$

称 $\boldsymbol{g}_\alpha$ 为**承載参数 $\beta_\alpha$ 的矢量**。在 (2.1) 中把足碼 $ij$ 看做二位数,按其大小順序排列,重新給予自然編碼,便得到形状 (2.2)。这时,若按足碼 $i$ 的大小順序把 $Y_i$ 排成 $v$ 行 $b$ 列,則承載 $\alpha_r$ 的矢量的正交分量中只有第 $r$ 行为 1,其余全为 0;承載 $\beta_c$ 的矢量的正交分量中只有第 $c$ 列为 1,其余全为 0. 在下面假設随机变数 $Z_1$, $Z_2, \cdots, Z_N$ 具有均值 0 和方差 $\sigma^2$,并且独立地分布,若无特别声明

---

❶ 本节包含一些新内容,討論非正交性的 BIB 設計的优点,是原著者在編写本书时得到的。——譯者注

时，并不假設它們遵循正态分布。

在很多情形中，通常按下列形式进行：

$$\alpha_2-\alpha_1,\quad (\alpha_1+\alpha_2)/2-\alpha_3,\quad (\alpha_1+\alpha_2)/2-(\alpha_3+\alpha_4+\alpha_5)/3,$$

所以一般設

$$\theta=l_1\beta_1+l_2\beta_2+\cdots+l_p\beta_p,\quad l_1+l_2+\cdots+l_p=0,\qquad (2.4)$$

并称 $\theta$ 为参数 $\beta_\alpha$ 間的**对比**。当用观察値的一次式

$$t=c_1Y_1+c_2Y_2+\cdots+c_NY_N=\mathbf{c}\cdot\boldsymbol{Y}\qquad (2.5)$$

来估計 $\theta$ 时，若其数学期望

$$E\{t\}=m_t=\theta,\qquad (2.6)$$

則称 $t$ 为 $\theta$ 的**无偏估計量**。若 $t$ 的方差

$$E\{(t-m_t)^2\}=\sigma_t^2\qquad (2.7)$$

为最小，則称 $t$ 为 $\theta$ 的**有效估計量**。无偏性与有效性兼备的估計量，叫做**最优估計量**❶。从无偏性的条件推出

$$\mathbf{c}\cdot\boldsymbol{g}_\alpha=l_\alpha\quad(\alpha=1,2,\cdots,p).\qquad (2.8)$$

若这样的 $\mathbf{c}$ 存在，則称 $\theta$ 为**可估的**。設

$$w_{\alpha\beta}\overset{\mathrm{d}}{=}\boldsymbol{g}_\alpha\cdot\boldsymbol{g}_\beta,\qquad (2.9)$$

令 $L_\beta$ 为联立方程

$$\sum_{\beta=1}^{p}w_{\alpha\beta}L_\beta=l_\alpha\qquad (2.10)$$

的任意一組解，并設

$$\mathbf{c}_p\overset{\mathrm{d}}{=}\sum_{\beta=1}^{p}L_\beta\boldsymbol{g}_\beta,\quad \mathbf{c}\overset{\mathrm{d}}{=}\mathbf{c}_p+\mathbf{c}_e,\quad \mathbf{c}_p\cdot\mathbf{c}_e=0,\qquad (2.11)$$

則 $t_0=\mathbf{c}_p\cdot\boldsymbol{Y}$ 是最优估計量。这可从下述看出：

$$\mathbf{c}_p\cdot\boldsymbol{g}_\alpha=\sum_{\beta=1}^{p}L_\beta\boldsymbol{g}_\beta\cdot\boldsymbol{g}_\alpha=l_\alpha,\qquad (2.12)$$

---

❶ 欲进一步深入，可参看 D. A. S. Fraser: Nonparametric Methods in Statistics (J. Wiley, New York, 1957).

$$\sigma_t^2=\mathbf{c}\cdot E\{(\boldsymbol{Y}-\boldsymbol{m})(\boldsymbol{Y}-\boldsymbol{m})\}\cdot\mathbf{c}=\mathbf{c}^2\sigma^2$$
$$=(\mathbf{c}_p+\mathbf{c}_c)^2\sigma^2\geqslant\mathbf{c}_p^2\sigma^2$$
$$=\Big(\sum_{\alpha=1}^{p}L_\alpha\boldsymbol{g}_\alpha\cdot\sum_{\beta=1}^{p}L_\beta\boldsymbol{g}_\beta\Big)\sigma^2$$
$$=(\sum_\alpha\sum_\beta w_{\alpha\beta}L_\alpha L_\beta)\sigma^2, \tag{2.13}$$

并且只有一个这样的 $\mathbf{c}_p$. 若 $\mathbf{c}_p\neq\mathbf{c}_p'$, 并且

$$t_0'=\mathbf{c}_p'\cdot\boldsymbol{Y}$$

也是最优估計量,則从无偏性推出

$$E(t-t')=0=(\mathbf{c}_p-\mathbf{c}_p')\cdot E\{\boldsymbol{Y}\}.$$

上式意味着 $\mathbf{c}_p-\mathbf{c}_p'$ 正交于 $\boldsymbol{g}_1, \boldsymbol{g}_2, \cdots, \boldsymbol{g}_p$ 所張成的空間, 但从(2.11)不难看出,本来 $\mathbf{c}_p$ 和 $\mathbf{c}_p'$ 就属于 $\boldsymbol{g}_1, \boldsymbol{g}_2, \cdots, \boldsymbol{g}_p$ 所張成的空間。这是矛盾。对給定的 $\boldsymbol{g}_\alpha$, (2.13)的右边給出最优估計量的方差,而若 $\boldsymbol{g}_\alpha$ 的方向或者大小可加以調整,則能使 $\sigma_t^2$ 变得更小。对(2.4)右边的 $l_\alpha$ 乘上一常数 $K$, 則(2.13)的右边变成 $K^2$ 倍,因此我們考慮

$$\sigma_t^2/(l_1^2+l_2^2+\cdots+l_p^2)\stackrel{\mathrm{d}}{=}\sigma^2 Q, \tag{2.14}$$

此处 Rayleigh 商

$$Q\stackrel{\mathrm{d}}{=}\sum_\alpha\sum_\beta w_{\alpha\beta}L_\alpha L_\beta/\sum_\alpha l_\alpha^2. \tag{2.15}$$

若对 $l_\alpha$ 作适当的正交变换,則(2.15)变成形状

$$Q=\sum_\alpha\mu_\alpha\xi_\alpha^2/\sum_\alpha\mu_\alpha^2\xi_\alpha^2, \tag{2.16}$$

此处 $\mu_\alpha$ 是 $\boldsymbol{w}\stackrel{\mathrm{d}}{=}(w_{\alpha\beta})$ 的特征方程

$$\sum_{\beta=1}^{p}w_{\alpha\beta}x_\beta=\mu x_\alpha \tag{2.17}$$

的特征根并满足

$$|w_{\alpha\beta}-\mu\delta_{\alpha\beta}|=0, \tag{2.18}$$

此处 $\delta_{\alpha\beta}$ 是 Kronecker 記号，即当 $\alpha=\beta$ 时为 1，$\alpha\neq\beta$ 时为 0。令 $\mu_0$ 表示特征根中非零的最小根，则从(2.16)显然有

$$Q\leqslant 1/\mu_0. \tag{2.19}$$

在(2.19)中等号至少对一个特定的 $l_1, l_2, \cdots, l_p$ 必成立。因此，我們想設法取 $\mu_0$ 尽可能地大，使得 $Q$ 的最大值尽可能地趋小。这相当于决定 $\boldsymbol{g}_\alpha$ 使得 $l_\alpha$ 的平方和导致一定对比的方差中最大的那个尽可能地趋小。

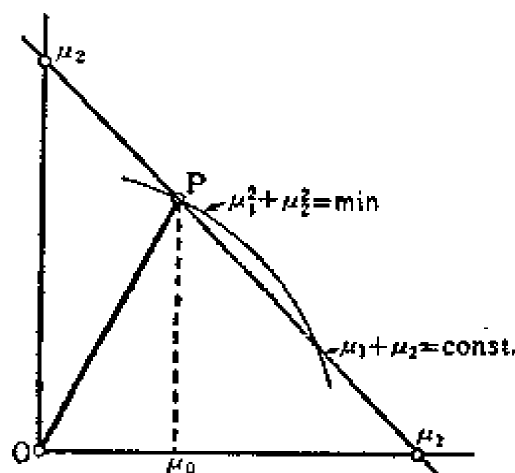



图 2.1

因为 $\boldsymbol{w}$ 的特征根之和是

$$\operatorname{tr}\boldsymbol{w}=\sum_{i=1}^{p}\mu_i=\sum_{\alpha=1}^{p}\boldsymbol{g}_\alpha^2, \tag{2.20}$$

特征根的平方和是

$$\operatorname{tr}\boldsymbol{w}^2=\sum_{i=1}^{p}\mu_i^2=\sum_{\alpha=1}^{p}\sum_{\beta=1}^{p}(\boldsymbol{g}_\alpha\cdot\boldsymbol{g}_\beta)^2, \tag{2.21}$$

所以当(2.20)为一定时，极小化(2.21)，$\mu_0$ 就成为最大。下面我們将利用这个事实。

(i) $\boldsymbol{g}_\alpha^2=a_\alpha^2(>0)\ (\alpha=1, 2, \cdots, p)$ 为一定，而且 $\boldsymbol{g}_\alpha$ 的方向可以調整的情形。

$$\operatorname{tr}\boldsymbol{w}=\sum_{\alpha=1}^{p}a_\alpha^2=\text{const}, \tag{2.22}$$

$$\operatorname{tr}\boldsymbol{w}^2=\sum_{\alpha=1}^{p}a_\alpha^4+2\sum_{\alpha<\beta}\sum(\boldsymbol{g}_\alpha\cdot\boldsymbol{g}_\beta)^2\geqslant\sum_{\alpha=1}^{p}a_\alpha^4. \tag{2.23}$$

上式中等号成立的充分条件是

$$w_{\alpha\beta}=\boldsymbol{g}_\alpha\cdot\boldsymbol{g}_\beta=0\quad(\alpha\neq\beta), \tag{2.24}$$

但这不一定是必要条件❶。(2.24)成立的情形，叫做**正交設計**。多因子試験(§13)就是它的一个应用例子。

〔注〕❶ 令 $\bar{\mu}$ 表示 $\boldsymbol{w}$ 的非零的特征根的平均，$p-d$ 为 $\boldsymbol{w}$ 的秩。若 $p>d+1$，则設

$$\sigma_\mu^2 \stackrel{d}{=} [\mathrm{tr}\,\boldsymbol{w}^2-(\mathrm{tr}\,\boldsymbol{w})^2/(p-d)]/(p-d-1).$$

由于 $\mathrm{tr}\,\boldsymbol{w}$ 为一定，所以极小化 $\sigma_\mu^2$ 对应于极小化 $\mathrm{tr}\,\boldsymbol{w}^2$。又記

$$\mu_0 \geqslant \bar{\mu} - \mathrm{const}\,\sigma_\mu, \tag{*}$$

则上式中的常数为正，并且关于 $\boldsymbol{w}$ 的非零特征根 $\mu$，$(\mu-\bar{\mu})^2$ 仅由依大小顺序排列后的 $(\mu_0-\bar{\mu})^2$ 的顺号及 $(p-d)$ 而定([7], p. 90)。但因(*)包含着不等号，所以除

$$\sigma_\mu=0$$

的情形以外，这不一定等于极大化 $\mu_0$。因此，(2.24)是充分条件，但不一定是必要条件。令 $a_0^2$ 为 $a_\alpha^2$ 中非零的最小的那个，則

$$\mu_0 \leqslant a_0^2,$$

所以，必要与充分条件是，$\boldsymbol{g}_0$ 被包含于 $\mu_0$ 的特征矢量所張成的空間中。(*)中的等号只能在这个場合成立。由此推出

$$w_{0\beta}=0 \quad (\beta\neq 0).$$

当(2.22)成立，以及 $a_\alpha^2$ 的大小可以調整的情形。

$$\sum_{\alpha=1}^{p} a_\alpha^4=\sum_{\alpha=1}^{p}(a_\alpha^2-a^2)^2+pa^4 \geqslant pa^4, \tag{2.25}$$

此处設

$$pa^2 \stackrel{d}{=} a_1^2+a_2^2+\cdots+a_p^2=\mathrm{tr}\,\boldsymbol{w}. \tag{2.26}$$

(2.25)中的等号当且仅当

$$\boldsymbol{g}_\alpha^2=a_\alpha^2=a^2 \tag{2.27}$$

时成立。这种情形，叫做**最优正交設計**。由正交陣列表(§14)产生的設計，就是它的一个例子。

(ii) $\boldsymbol{g}_\alpha$ $(\alpha=1, 2, \cdots, r<p)$ 固定，而且只有 $\boldsymbol{g}_\beta$ $(\beta=r+1,$

❶ 这个"注"是根据原著者的訂正譯出的。在原书中著者以为(2.24)是必要与充分条件。——譯者注

$r+2, \cdots, p$) 的方向可以調整的情形。由于(2.22)成立，所以在(2.23)中令

$$w_{\alpha\beta}=\boldsymbol{g}_\alpha\cdot\boldsymbol{g}_\beta=0, \quad \left.\begin{array}{l}\alpha=1, 2, \cdots, r, \\ \beta=r+1, r+2, \cdots, p,\end{array}\right\} \tag{2.28}$$

則 $\operatorname{tr} \boldsymbol{w}^2$ 为最小。

$\boldsymbol{g}_\beta$ ($\beta=r+1, r+2, \cdots, p$) 的大小可以調整的情形，在极值問題中去掉約束条件，則极小值不会大，所以只須使 $\boldsymbol{g}_\beta^2=a_\beta^2$ 的大小不小于

$$(w_{\alpha\beta}), \quad \alpha, \beta=1, 2, \cdots, r \tag{2.29}$$

的最小特征根即可。

(iii) 不完全設計的情形。在(2.1)中令 $\boldsymbol{g}_i$ 为承戴 $\alpha_i$ 的矢量，$\boldsymbol{h}_j$ 为承戴 $\beta_j$ 的矢量，則

$$E\{\boldsymbol{Y}\}=\sum_{i=1}^{v}\alpha_i\boldsymbol{g}_i+\sum_{j=1}^{b}\beta_j\boldsymbol{h}_j. \tag{2.30}$$

又令

$$\boldsymbol{g}_i^2=r_i, \quad \boldsymbol{h}_j^2=k_j, \quad \boldsymbol{g}_i\cdot\boldsymbol{h}_j=n_{ij} \tag{2.31}$$

分別表示品种 $V_i$ 的实施数，区組 $B_j$ 的大小和結合矩陣第 $i$ 行第 $j$ 列的元素。一般，$B_j$ 包含 $V_i$ 的次数为 $n_{ij}$。

$$\boldsymbol{d}_i\overset{d}{=}\boldsymbol{g}_i-\sum_{j=1}^{b}(\boldsymbol{g}_i\cdot\boldsymbol{h}_j)\boldsymbol{h}_j/\boldsymbol{h}_j^2 \tag{2.32}$$

是属于 $\boldsymbol{g}_i$ 但不属于 $\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_b$ 所張成空間的矢量，而

$$P_i\overset{d}{=}\boldsymbol{d}_i\cdot\boldsymbol{Y} \tag{2.33}$$

是从 $\boldsymbol{g}_i\cdot\boldsymbol{Y}$ 中把試驗場所引起的偏差，即把区組效应消去后的效应❶。設

$$\boldsymbol{d}_i\cdot\boldsymbol{d}_j=r_i\delta_{ij}-\sum_{l=1}^{b}n_{il}n_{jl}/k_l\overset{d}{=}c_{ij}=c_{ji}, \tag{2.34}$$

❶ 参看 Bose [1]，第3章§2以下，或者增山[8]，注17。

又令

$$\theta \stackrel{\mathrm{d}}{=} l_1\alpha_1 + l_2\alpha_2 + \cdots + l_v\alpha_v \tag{2.35}$$

为品种效应間的对比，则相当于(2.10)的有

$$\sum_{j=1}^{v} c_{ij} p_j = l_i, \tag{2.36}$$

并且 $\theta$ 的最优估計量由

$$t = \sum_{i=1}^{v} p_i P_i \tag{2.37}$$

給出，它的方差为

$$\sigma_t^2 = \left(\sum_{i=1}^{v}\sum_{j=1}^{v} c_{ij} p_i p_j\right)\sigma^2. \tag{2.38}$$

根据 König 的想法，如果从表示任一品种的白球到表示另外的任一品种的白球的色綫徑路存在，那末这种設計叫做**完全連結型**，并且不带区組引起的偏差可以估計品种效应間的任意对比。这时，矩陣 $\boldsymbol{u} \stackrel{\mathrm{d}}{=} (c_{ij})$ 的秩为 $v-1$，而且特征方程

$$\sum_{j=1}^{v} c_{ij} x_j = \mu x_i \tag{2.39}$$

有单根 $\mu=0$。这个特征根的特征矢量是 $x_j=1$ $(j=1, 2, \cdots, v)$，把它們代入上式，便有

$$\sum_{j=1}^{v} c_{ij} = 0 \quad (i=1, 2, \cdots, v). \tag{2.40}$$

这时我們有

$$\mathrm{tr}\,\boldsymbol{u} = \sum_{i=1}^{v} \mu_i = \sum_{i=1}^{v} c_{ii} = N - \sum_{i=1}^{v}\sum_{l=1}^{b} n_{il}^2/k_l. \tag{2.41}$$

在上式中設❶

$$n_{il}^2 = n_{il}, \quad k_l = k, \tag{2.42}$$

并若試験总数 $N$ 和区組个数 $b$ 为一定，则

---

❶ 后来森口繁一放寬这个假定，即令 $n_{il}^2 \geqslant n_{il}$，$k_l \leqslant k$，并使 $N$，$v$，$k$ 为一定，也得到同一的結果。

$$\mathrm{tr}\,\boldsymbol{u}=N-b=\text{const}. \tag{2.43}$$

这时我們有

$$c_{ii}=r_i(1-1/k),\quad c_{ij}=-\lambda_{ij}/k\quad(i\neq j), \tag{2.44}$$

所以

$$\mathrm{tr}\,\boldsymbol{u}^2=\sum_{i=1}^{v}\sum_{j=1}^{v}c_{ij}^2=(1-1/k)^2\sum_{i=1}^{v}r_i^2+2\sum_{i<j}\sum\lambda_{ij}^2/k^2. \tag{2.45}$$

对 $r_i$ 的約束条件是

$$\sum_{i=1}^{v}r_i=N, \tag{2.46}$$

从(2.40)和(2.44)推出，对 $\lambda_{ij}$ 的約束条件是

$$r_i(k-1)-\sum_{j=1}^{v}{}'\lambda_{ij}=0. \tag{2.47}$$

此处 $\sum$ 上角的‘$'$’表示除掉 $j=i$ 的情形。在上列两个約束条件下，极小化(2.45)便得到

$$r_i=\text{const}\,(\overset{\mathrm{d}}{=}r),\quad \lambda_{ij}=\text{const}\,(\overset{\mathrm{d}}{=}\lambda), \tag{2.48}$$

$$\lambda=r(k-1)/(v-1). \tag{2.49}$$

这无非是 BIB. 令 $\bar{\mu}$ 表示 $\boldsymbol{u}$ 的非零特征根的平均，$\overline{\mu^2}$ 表示特征根平方的平均，則

$$\mathrm{tr}\,\boldsymbol{u}=b(k-1)=(v-1)\bar{\mu}, \tag{2.50}$$

$$\begin{aligned}\mathrm{tr}\,\boldsymbol{u}^2&=vr^2(1-1/k)^2+v(v-1)\lambda^2/k^2\\&=b^2(k-1)^2/(v-1)\\&=(v-1)\overline{\mu^2}.\end{aligned} \tag{2.51}$$

故得

$$\bar{\mu}^2=\overline{\mu^2}. \tag{2.52}$$

从而又得

$$\bar{\mu}=\mu_0. \tag{2.53}$$

若对固定的 $\lambda_{ij}$ 极小化 $\mathrm{tr}\,\boldsymbol{u}^2$，則只得出 $r_i=r$. 部分平衡不完全区組(PBIB)就是它的特殊情形(增山元三郎，1957)。

我們在(2.1)或者(2.30)中对于試驗場所引起的偏差，只考慮了它的一个方向。这叫做**一方約束型**。如 Youden 方的情形那样，考慮两方向的，叫做**两方約束型**。在这个場合，考慮 $k(\leqslant v)$ 行和 $b(\geqslant v)$ 列的区組，并令第 $r$ 行第 $c$ 列包含品种 $V_i$，则可考慮构造模型

$$E\{\boldsymbol{Y}\}=\sum_{i=1}^{v}\alpha_i\boldsymbol{g}_i+\sum_{r=1}^{k}\beta_r\boldsymbol{h}_r+\sum_{c=1}^{b}\beta'_c\boldsymbol{h}'_c, \tag{2.54}$$

此处 $\beta_r$ 和 $\beta'_c$ 分别表示第 $r$ 行和第 $c$ 列的区組效应。令 $n_{ir}$ 表示 $V_i$ 被包含于 $r$ 行的次数，$n'_{ic}$ 表示 $V_i$ 被包含于 $c$ 列的次数，则 $V_i$ 的实施数是

$$r_i=\sum_{r=1}^{k}n_{ir}=\sum_{c=1}^{b}n'_{ic}. \tag{2.55}$$

若区組无空地被利用，则試驗总数是

$$N=bk=\sum_{i=1}^{v}r_i. \tag{2.56}$$

設

$$\lambda_{ij}\stackrel{\mathrm{d}}{=}\sum_r n_{ir}n_{jr}\quad(i\neq j),\quad \lambda'_{ij}\stackrel{\mathrm{d}}{=}\sum_c n'_{ic}n'_{jc}\quad(i\neq j). \tag{2.57}$$

如一方約束型的情形那样进行，便得到❶相当于(2.34)的 $c_{ij}$，

$$c_{ii}=r_i\{1+r_i/(bk)\}-\sum_r n_{ir}^2/b-\sum_c n'^2_{ic}/k, \tag{2.58}$$

$$c_{ij}=r_ir_j/(bk)-\lambda_{ij}/b-\lambda'_{ij}/k\quad(i\neq j). \tag{2.59}$$

設

$$S_i\stackrel{\mathrm{d}}{=}\sum_r n_{ir}^2-(\sum_r n_{ir})^2/k, \tag{2.60}$$

则

$$\mathrm{tr}\,\boldsymbol{u}=\sum_{i=1}^{v}c_{ii}=N-\sum_i S_i/b-\sum_i\sum_c n'^2_{ic}/k \tag{2.61}$$

$$\leqslant N-\sum_i\sum_c n'^2_{ic}/k \tag{2.62}$$

$$\leqslant N(1-1/k)=b(k-1). \tag{2.63}$$

❶ 参看 Bose [1]，第3章 §12，增山[8]，注17。

在(2.62)中等号当且仅当

$$S_i=0 \text{ 或者 } n_{ir}=m_i(\text{不依赖于 } r) \tag{2.64}$$

时成立，而在(2.63)中等号当且仅当

$$n'^2_{ic}=n'_{ic} \tag{2.65}$$

亦即 $n'_{ic}$ 为 1 或者 0 时成立。因此，在給定的条件下，如后述那样，当

$$\text{tr}\, \boldsymbol{u}=b(k-1) \tag{2.66}$$

时，$\mu_0$ 可能成为最大。在这个場合，我們有

$$c_{ii}=m_i(k-1), \quad c_{ij}=-\lambda'_{ij}/k \quad (i\neq j), \tag{2.67}$$

$$r_i=\sum_r n_{ir}=km_i, \tag{2.68}$$

$$\sum_i r_i=kb=k\sum_i m_i \quad \text{或者} \quad \sum_i m_i=b, \tag{2.69}$$

$$\text{tr}\, \boldsymbol{u}^2=\sum_i\sum_j c_{ij}^2=(k-1)^2\sum m_i^2+2\sum_{i<j}\sum(\lambda'_{ij})^2/k^2. \tag{2.70}$$

若只考虑完全連結型的情形，則 $\boldsymbol{u}$ 的秩是 $v-1$. 如一方約束型那样，极小化 $\text{tr}\, \boldsymbol{u}^2$，便得到

$$m_i=m \quad (\text{不依赖于 } i), \tag{2.71}$$

$$\lambda'_{ij}=\lambda \quad (\text{不依赖于 } i, j). \tag{2.72}$$

故得

$$\sum_i m_i=mv=b. \tag{2.73}$$

这时，从极小化的条件又导出

$$\lambda=km(k-1)/(v-1)=r(k-1)/(v-1), \tag{2.74}$$

設

$$\text{tr}\, \boldsymbol{u}=b(k-1)=(v-1)\bar{\mu}, \tag{2.75}$$

則

$$\begin{aligned}\text{tr}\, \boldsymbol{u}^2&=v(k-1)^2m^2+v(v-1)\lambda^2/k^2\\&=v^2(k-1)^2m^2/(v-1)\\&=(v-1)\bar{\mu}^2.\end{aligned} \tag{2.76}$$

因此，(2.52) 自动地成立。在上式中特别令 $m=1$，则这是 §1 的 Youden 方，令 $m=1$ 并且 $v=k$，则这是 §14 的拉丁方。若 $m>1$，则一般叫做 **Shrikhande 方** (S. S. Shrikhande, 1951) ❶ (增山元三郎，奥野忠一，1957)。

无論是一方約束的情形或者是两方約束的情形，我們都有

$$\mu_0=\bar{\mu}=b(k-1)/(v-1)=v\lambda/k\overset{\mathrm{d}}{=}rE. \tag{2.77}$$

上式的 $E$ 叫做**效率因子**。若 $v>k$，則 $E<1$. 如果区組差不存在❷，那末两个品种各重复 $r$ 次的平均收成之差的方差是 $2\sigma^2/r$，但是在 BIB, Youden 方以及 Shrikhande 方中則是 $2\sigma^2/\mu_0=2\sigma^2/rE$. 因此，比較的精度降低为 $E$ 倍。但是在区組差存在的情形，通过随机化把这个差处理为随机变数，这等于使 $\sigma$ 趋大，所以若不討厌計算上的或多或少的麻煩，則可以适当地把区組分得小些，使得能够在区組内保存試驗条件的均勻性。

回到一方約束型上去。相当于(2.11)的是

$$\mathbf{c}_0\overset{\mathrm{d}}{=}\sum_{i=1}^{v}p_i\boldsymbol{d}_i, \tag{2.78}$$

从而有

$$E\{t\}=\theta=\sum p_i\boldsymbol{d}_i\cdot E(\boldsymbol{Y})=\sum p_i\boldsymbol{d}_i\cdot\sum \boldsymbol{a}_j\boldsymbol{d}_j=\mathbf{c}_0\cdot\sum\boldsymbol{a}_j\boldsymbol{d}_j. \tag{2.79}$$

因此，設

$$\psi^2\overset{\mathrm{d}}{=}(\sum a_j\boldsymbol{d}_j)^2/[(v-1)\sigma^2], \tag{2.80}$$

則从 Cauchy 不等式推出

$$(v-1)\mathbf{c}_0^2\psi^2\sigma^2=(v-1)\psi^2\sigma_t^2\geqslant\theta^2. \tag{2.81}$$

故使 $\sigma_t^2$ 趋小相应于使 $\psi^2$ 趋大。若假定 $Z_i$ 的正态性，則在方差分析中作 $F$ 檢驗时，消去区組效应后的品种摆动的檢驗功效函数是

❶ Shrikhande[52]. ——譯者注

❷ 即指完全区組的情形。——譯者注

$\psi^2$ 的单增函数，而若其他情况不变，則 $\psi^2$ 越大，忽視品种間差异的冒險率就越小。

## §3 組合方法

一般，把 $v$ 个品种安排在大小为 $k$ 的区組中，使得特定的 $\beta$ 个品种在同一区組相遇 $\alpha$ 次，这种情形叫做**完全 $\alpha$-$\beta$-$k$-$v$ 的战术构形**。这个奇怪的名称，恐怕是由与下述 Euler 方問題(§14)的类似性产生出来的。Euler 問題是❶，能否从 6 个連队抽出 6 种軍銜的軍官各一人，共 36 人，排成 6 行 6 列，使得每行每列都有各連队和各軍銜的代表？特别，$\alpha=1$ 的情形，叫做 **Steiner 系**，因为 J. Steiner (1853) ❷❸，在研究 4 次曲綫的 2 重切綫时曾經处理过这种問題。尤其对 $k=3$ 的**三点系**，人們作了較多的研究❹。当 $\alpha=1$ 时，令 $\gamma(\beta, k, v)$ 表示 Steiner 系。显然，一般的完全战术构形給出一个 BIB，此处

$$v=v,\quad k=k,\quad b=\alpha\,{}_vC_\beta/{}_kC_\beta,\quad r=\alpha\,{}_{v-1}C_{\beta-1}/{}_{k-1}C_{\beta-1},$$

$$\lambda=\begin{cases}\alpha\,{}_{v-2}C_{\beta-2}/{}_{k-2}C_{\beta-2}, & \beta\geqslant 3,\\ \alpha, & \beta=2.\end{cases}\tag{3.1}$$

(3.1)是任意 $u$ 个品种的相遇数，因为(3.1)等于除这些 $u$ 个以外的 BIB 的区組个数

$$\lambda_u=\alpha\,{}_{v-u}C_{\beta-u}/{}_{k-u}C_{\beta-u}.\tag{3.2}$$

附表 1 中的記号 $U$ 表示由这个方法对 $k=\beta$ 和 $\alpha=1$ 可以构

---

❶ 参看刘璋温[35]。——譯者注

❷ E. Pascal: Repertorium der höheren Mathematik II, 1. Geometrie (Teubner, Leipzig, 1910), 408.

❸ Steiner [58]。——譯者注

❹ E. Netto: Lehrbuch der Combinatorik (Teubner, Leipzig, 1927), 202. 以后的进一步的研究，見 E. Witt: Abh. math. Seminar Univ. Hamburg, 12 (1938), 265～275.

造的 BIB. 特别,令 $k=v-1$, 则得到 SBIB. $v\leqslant 5$ 的 BIB 只能由这个方法来构造,但对 $v>6$ 则还存在着由这个方法以外的 BIB.

**例 1** 对 $v=6$, $k=3$ 的情形, 从 (0 1 2) 出发, 按辞典方式作 (0 1 3), (0 1 4),…, (3 4 5) 就可以写下 $b=20$ 个区組,而其实仅其中的一半:

(0 1 2) (0 1 4) (0 2 3) (0 3 5) (0 4 5)

(1 2 5) (1 3 4) (1 3 5) (2 3 4) (2 4 5)

也是一个 BIB. 效率因子都是 4/5.

这个例子表明,当給定 $v$ 与 $k$ 时,区組个数 $b$ 比組合方法来得小的 BIB 可能存在。我們将研究在什么样的場合这是可能的。就設計而論,基本关系由結合矩陣規定,而問題只是称为品种的第一类东西与称为区組的第二类东西的結合关系。因此,把第一类东西称为点,第二类东西称为直綫也罢,或者把第一类东西称为多面体的棱,第二类东西称为多面体的面也罢,这都不要紧❶。把第一类东西称为点,第二类东西称为固有二次曲面也行❷。下面对具体地求解,我們利用几何方法,而对求解的存在条件,则利用代数方法。当然,严格的区别是有困难的,求解的方法也可以說是利用几何代数方法。

## §4 平面有限射影几何 $PG[2,t]$

为了証明几何学公理系的无矛盾性及公理相互間的独立性,自 19 世紀以来开始形成了一种看来奇怪的几何学。当时这种几何学的意义就是那么些,但是在本世紀 20 年代試驗設計法产生以后,这种奇怪几何中的有限个元素的集合被积极地用来求满足給定条件的試驗設計。下面我們把第一类东西称为**点**,第二类东西称为**直綫**,并置下列**結合公理**。

---

❶ Levi[5].

❷ Levi[5],至于利用球面以及双曲面的情形,可参看前頁脚注 E. Witt 的文献。

$PG_2.1$ 必存在而且只存在一条直綫結合着不同两点 $A$ 和 $B$。記作 $A\cup B$ 或者 $AB$。(∪ 表示 unite 的 u)

$PG_2.2$ 必存在而且只存在一点結合着不同两条直綫 $a$ 和 $b$。記作 $a\cap b$。(∩ 表示 meet 的 m 的一部分)

$PG_2.3$ 各点至少結合着三条不同直綫。

$PG_2.4$ 各直綫至少結合着三个不同点。

这里，若把点与直綫这两个詞交换，則只有公理号碼变更而公理系本身不发生变化。因此，在从这个公理系得到的定理中，把点与直綫对换后，定理仍然成立。这叫做**对偶原理**。只要把这一点弄清楚，然后把結合这个詞改为常用語也不要紧。例如，$PG_2.1$ 可以改为存在一条直綫通过两点 $A$ 和 $B$；$PG_2.2$ 可以改为存在两条直綫 $a$ 和 $b$ 的一个交点，等等。从公理系的純粹性来說，可以把 $PG_2.2$ 改为"不同两条直綫至少交于一点"，并用 $PG_2.1$ 来証明只能交于一点；以及把 $PG_2.3$, 4 改为"存在四点其中任意三点不在同一条直綫上"，但是为了便于理解对偶原理，我們忽視了純粹性。

在普通的 Euclid 平面上，不同两条直綫要么相交，要么平行，而且通过直綫外一点只有一条直綫与这条直綫平行。如果在各直綫上添加**无限远点**，把这些无限远点全体定义为在一条**无限远直綫**上，并規定平行的两条直綫公有无限远点，那末任意两条不同的直綫必相交于一点，因而沒有必要去特別考慮平行綫。若用画法几何学上的透視图法进行射影，則在一平面上平行的两条直綫在別的平面上就变为相交。利用"射影"这个术語，把无限远直綫和其上的点加起来而成的扩大平面叫做**射影平面**。在这个意义下，把上列四个公理叫做**射影几何**($PG$)**的公理**。

下面特別考慮点的总数 $v$ 为有限的情形。

令 $a$, $b$ 表示任意两条不同的直綫，則存在第三条直綫 $c$ 通过它們的交 $A=a\cap b$。在 $c$ 上存在着既不在 $a$ 又不在 $b$ 上的点 $C$。

因为在直綫 $a$ 上只存在有限个点，所以設它們为

$$k \stackrel{d}{=} t+1=(t^2-1)/(t-1). \tag{4.1}$$

考虑这些点中的各点与 $C$ 結合的直綫，則这些直綫只能与 $b$ 相交一次，并且必与 $b$ 交于互不相同的点上。故在 $b$ 上至少有 $k$ 个点。若在 $b$ 上有多于 $k$ 个点，則这些点与 $C$ 結合的直綫必与 $a$ 交于前述 $k$ 个以外的点上。因这不可能，所以在 $b$ 上不存在多于 $k$ 个点。同理可知，每条直綫都有 $k$ 个点。

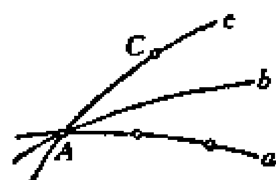



图 4.1

从对偶原理推出，在同一点上相交的不同直綫的个数是

$$r=t+1. \tag{4.2}$$

因为必存在一条直綫把平面上任意的点和 $A$ 結合在一起，所以为了計算平面上的点的个数，只要計算通过点 $A$ 的直綫上的点的个数即可。除点 $A$ 以外各直綫上有 $t$ 个点，而且通过 $A$ 的直綫有 $t+1$ 条，所以除点 $A$ 以外总共有 $t(t+1)$ 个点。因此，不同点的总数是

$$v=t(t+1)+1=t^2+t+1=(t^3-1)/(t-1). \tag{4.3}$$

从对偶原理推出，不同直綫的总数是

$$b=t^2+t+1. \tag{4.4}$$

根据 $PG_2.1$，通过特定不同两点的直綫个数是

$$\lambda=1. \tag{4.5}$$

故若一条直綫上有 $t+1$ 个点的 $PG$ 存在，則得到

$$\left.\begin{array}{c} v=b=t^2+t+1,\ k=r=t+1,\ \lambda=1, \\ E=(t^2+t+1)/(t+1)^2 \end{array}\right\} \tag{4.6}$$

的 SBIB. 如 § 8 所述，若 $t$ 是素数或素数冪，則 $PG$ 必存在，但如 § 15 所述，对 $t=6$, 14, 21 等情形，滿足上列公理系的 $PG$ 則不存在。人們猜想，对 $t=10$, 18, 20 等情形恐怕也不存在。以

$PG[2, t]$ 表示一直綫上有 $t+1$ 个点的平面有限射影几何。

**例1** 把§1的例1表如图4.2。在△0 1 2的頂点分别放上质量 $g_1$, $g_2$, $g_3$,并令$[g_1, g_2, g_3]$表示重心位置。令3, 4和6分别表示0 1, 1 2和2 0的中点,5表示重心,则得表4.1。在这个 Möbius 重心坐标中,若 $\rho\neq0$,则

$$[g_1, g_2, g_3]=[\rho g_1, \rho g_2, \rho g_3],$$

所以有例如

$$([1\ 0\ 0]+[0\ 1\ 0])/2=[1\ 1\ 0].$$

与§1的表1.1比較一下,可知图的虚綫也应看做"一条直綫"。

$$([1\ 1\ 0]+[0\ 1\ 1])/2=[1\ 2\ 1].$$

这相当于承认[1 2 1]和[1 0 1]为同一点。若以 $\left.\begin{matrix}0\ 1\\2\ 5\end{matrix}\right\}3$ 表示直綫 0 1 和 2 5 的交点为3,并按这种記法,以0, 1, 2, 5为生成系,则得其他点如:

$$\left.\begin{matrix}0\ 1\\2\ 5\end{matrix}\right\}3 \qquad \left.\begin{matrix}1\ 2\\0\ 5\end{matrix}\right\}4 \qquad \left.\begin{matrix}2\ 0\\1\ 5\end{matrix}\right\}6 \qquad \Big|3\ 4\ 6$$

右侧的纵綫表示,右侧的三点在同一直綫上。这就是在每一直綫上各有三点而总共有七点的构形,依这个意义以記号 $v_k=7_3$ 来表示❶。

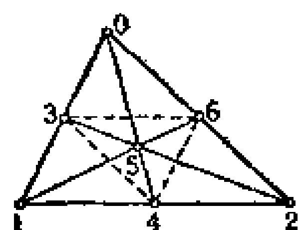


图 4.2

表 4.1

| 点 | 重心坐标 | | |
|---|---|---|---|
| 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 |
| 2 | 0 | 0 | 1 |
| 3 | 1 | 1 | 0 |
| 4 | 0 | 1 | 1 |
| 5 | 1 | 1 | 1 |
| 6 | 1 | 0 | 1 |

## §5 有限射影几何 $PG[s, t]$

O. Veblen 和 W. H. Bussey (1906) ❷用 $PG[s, t]$表示一直

❶ F. Levi: Geometrische Konfigurationen (Hirzel, Leipzig, 1929). D. Hilbert und S. Cohn-Vossen: Anschauliche Geometrie (Springer, Berlin, 1932).

❷ Veblen-Bussey [61].——譯者注

綫上有 $t+1$ 个点的 $s$ 維空間的射影几何,并用下列公理系規定之。

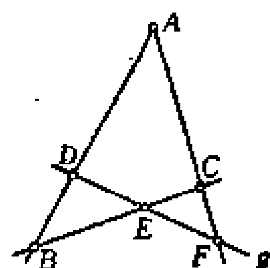


图　5.1

$PG.1$　集合 $PG$ 由有限个不同点組成,包含被称为直綫的集合为子集。直綫至少由三点組成。

$PG.2$　必存在而且只存在一条直綫 $AB$ 結合着不同两点 $A$ 和 $B$。

$PG.3$　令 $C$ 为不在直綫 $AB$ 上的一点。若直綫 $g$ 包含 $AB$ 上不同于 $A$, $B$ 的点 $D$, 又包含 $BC$ 上不同于 $B$, $C$ 的点 $E$,则 $g$ 包含 $CA$ 上的点 $F$.

$PG.4$　把点称为**零維空間**,直綫称为**一維空間**,平面称为**二維空間**,并令正整数 $m$ 小于正整数 $s$, 則不包含于 $m$ 維空間的点包含于 $s$ 維空間。

$PG.5$　在 $PG.4$ 的条件下,集合中不存在 $s+1$ 維空間。

若 $s\geqslant3$, $t\geqslant2$,則下列 **Desargues 定理**成立。从公理容易看出,这时有五点 1, 2, 3, 4, 5, 其中任意四点不在同一平面上。令 $O\overset{d}{=}(1\ 2)$, $A\overset{d}{=}(1\ 3)$和 $A'\overset{d}{=}(2\ 3)$分别表示1 2, 1 3 和 2 3 与某一平面 $\pi$ 的交点,則 $O$, $A$, $A'$ 在同一直綫(1 2 3)上。同样令 $O=(1\ 2)$, $B\overset{d}{=}(1\ 4)$和 $B'\overset{d}{=}(2\ 4)$分别表示 1 2, 1 4 和 2 4 与 $\pi$ 的交点,則 $O$, $B$, $B'$ 也在同一直綫 (1 2 4) 上。又令 $O=(1\ 2)$, $C\overset{d}{=}(1\ 5)$ 和 $C'\overset{d}{=}(2\ 5)$分别表示 1 2, 1 5 和 2 5 与 $\pi$ 的交点,則 $O$, $C$, $C'$ 也在同一直綫 (1 2 5) 上。这时 $AB$ 与 $A'B'$ 的交点 $X\overset{d}{=}(3\ 4)$, $BC$ 与 $B'C'$ 的交点 $Y\overset{d}{=}(4\ 5)$ 以及 $CA$ 与 $C'A'$ 的交点 $Z\overset{d}{=}(3\ 5)$在同一直綫(3 4 5)上。这就是說,如果連結 $\pi$ 上$\triangle ABC$

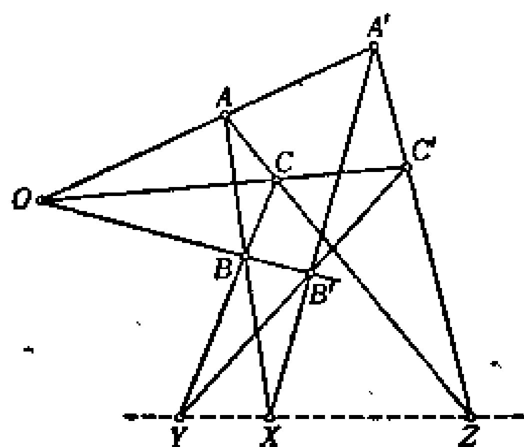


图　5.2

和 $\triangle A'B'C'$ 对应頂点的三直綫交于被称为**透視中心**的 $O$,那末对应对边的交点 $X$, $Y$ 和 $Z$ 在被称为**透視軸**的一直綫上。其逆也成立。若对应对边的交点在同一直綫上，則連結对应頂点的三直綫交于同一点。这是 **$10_3$ 的构形**。

这个定理对 $PG[2,t]$ 不一定成立[1]。因为在大于三維的空間中二直綫不一定相交，所以相交这个条件是个强条件。H. Ф. Четверхин.(1927) 取坐标集合 $\mathfrak{C}$ 为实数体，令$[x, y, z]$ 表示点，定义

当 $ab \geqslant 0$ 时，

$$ax+by-z=0 \quad (\text{第一类直綫}), \tag{5.1}$$

当 $\alpha\beta \leqslant 0$ 时，

$$\alpha x^3+\beta y^3+z^3=0 \quad (\text{第二类直綫}) \tag{5.2}$$

为直綫，証明了它們满足 §4 的 $PG_2$，并証明了当取九直綫为第一类直綫，剩下一直綫为第二类直綫时，Desargues 定理不成立。当然，事前要选擇系数，使得在第二类直綫上依普通意义不在同一直綫上的三点是頂点。

这个例子表明，不是多維射影空間的子空間的射影平面的存在性。关于这一点，将在下节作进一步的討論。

---

[1] D. Hilbert: Grundlagen der Geometrie (Teubner, Stuttgart, 1899, 1956). 在新版中已改为 Moulton 的簡单例子，而原来的例子可在米山国藏：数学の基础，上，积善館，1925 中找到。

# 第2章　不完全区組設計的构造

## §6 点　代　数[1]

設有两个平面，結合关系不变，而点与点，直綫与直綫是一一对应，則这两个平面叫做**同构**。从一平面到另一平面的对应，叫做**映射**。从一平面到另一平面的对应不一定是一一对应，但是一价时，叫做**同态**。又若一平面的点和直綫不变結合关系分別对应于另一平面的直綫和点，則称两平面为**对偶的**。使一平面同构地映射于其本身，叫做**直射变换**，使一平面对偶地映射于其本身，叫做**对射变换**。允許对射变换的平面，称为**自对偶的**。

若代替 $PG_2.1$ 而采用

$PG_2.1'$　至多有一条直綫結合着不同两点，因此至多只有一点結合着不同两条直綫，

則这些点和直綫的集合叫做**部分平面**或者**結合构造**(M. Hall, 1943)[2]。令 $\alpha_0$ 为这个平面上的点的个数，$\alpha_1$ 为直綫个数，$i$ 为点与直綫結合場合个数，則

$$r \overset{d}{=} 2(\alpha_0+\alpha_1)-i \tag{6.1}$$

叫做这个部分平面的**秩**(A. Копейкина, 1945)。按下列步驟，可把部分平面 $\pi_0$ 推广到完全平面 $\pi$. 首先把 $\pi_0$ 上的点叫做零次元素，而任意两个零次元素不为直綫結合的，用直綫結合它們。但这条綫不再結合另外的点。这叫做**自由开拓**。如此得到的直綫和原

---

[1] Artin [12]，第2章；Dubreil-Jacotin-Lesieur-Croisot [13]，第3部分。本节主要应归功于 Л. А. Скорняков: Проективные плоскости, УМН, 6 (1951), 112～154.

[2] Hall [80].——譯者注

来在 $\pi_0$ 上已有的直綫的全体,叫做一次元素。其次作仍未有交点的任意二直綫的交点。但这个交点只結合这两条直綫。这也叫做自由开拓。这些交点叫做二次点。設一次直綫和零次及二次点的全体为部分平面 $\pi_1$. 按完全相同的步驟，从 $\pi_1$ 得到包含四次元素的部分平面 $\pi_2$. …… 尽可能继續这种操作,便有

$$\pi_1 \cup \pi_2 \cup \pi_3 \cup \cdots = \pi. \tag{6.2}$$

这叫做**完全自由开拓**。这个开拓唯一决定。自由开拓的逆操作叫做**自由收縮**。从(6.1)不难看出，无論是 $\alpha_0$ 增加一个或是 $\alpha_1$ 增加一个，$i$ 都增加二个，所以秩或是自由开拓或是自由收縮而不变化。若依自由开拓或自由收縮，能从一个部分平面移到另一个部分平面，则称两个部分平面为**自由等价的**。

由有限个元素所成的部分平面，叫做二維构形。若构形 $\mathfrak{K}$ 同构地映射于平面 $\pi$ 的某一部分平面，则称 $\mathfrak{K}$ 在 $\pi$ **上实現**。如 §5 中的 Desargues 定理那样，下列形式的定理叫做**构形定理**:“若在平面 $\pi$ 上給定的某个构形 $\mathfrak{K}$，除一部分以外，所有的結合关系都实現，則其余部分的結合关系也实現”。

在由有限个元素所成的部分平面上，若任意直綫至少結合三点，任意一点至少結合三直綫，則称这个部分平面为**閉的**。任何部分的部分平面不为閉的部分平面称为**开的**。§4 的 $7_3$ 和 §5 的 $10_3$ 都是閉的。这里所謂**部分的部分平面**，乃是指由部分平面的点和直綫的一部或者全部所成而且它們之間的結合关系与原来的部分平面相同的平面。开的部分平面依自由开拓仍然是开的部分平面，所以与它等价的部分平面都是开的。取 $n$ 为大于等于 4 的整数，則任意一个开的部分平面自由等价于由結合 $n$ 个点与其中的 $(n-2)$ 个点的一直綫所成的部分平面，并且秩 $r$ 满足关系

$$n+4=r. \tag{6.3}$$

开的部分平面依自由开拓移到开的部分平面这个事实表明，

构形定理要在§5的 $PG$ 公理加上新的公理之后才能成立。当然，从一个构形定理也可导出另一个构形定理。例如 Pappus 定理(后面将提到)蘊涵 Desarguos 定理(G. Hessenberg, 1905)。

現在射影平面上引进坐标。任意三点不在同一直綫上的四点称为处于**一般位置**，或者形成**完全四点形**。設四点 $O$, $E$, $U$, $V$ 处于一般位置，給通过 $U$ 的直綫集合即**綫束**和通过 $V$ 的綫束以一一对应。当然，对一个綫束中的不同直綫給予不同号碼。对应方法，例如对交于 $OE$ 上同一点的 $U$ 的直綫和 $V$ 的直綫，給予相同号碼或者暗号。但 $UV$ 为例外。給 $UO$ 以号碼0，給 $UE$ 以号碼1．不在 $UV$ 上的任意一点 $P$ 的**坐标**，由 $UP$ 的号碼 $x$ 和 $VP$ 的号碼 $y$ 定为 $(x, y)$．若預先決定綫束的号碼，則坐标唯一决定，反之，若給定 $(x, y)$，則 $P$ 唯一决定。依定义，$OE$ 上的点的两坐标相等，$E$ 的坐标是 $(1, 1)$．$UV$ 上的任意一点 $Q$ 的坐标，若 $OQ$ 和 $UE$ 的交点坐标为 $(1, m)$，則設为 $(m)$．若要求整齐性，則应設为 $(\infty, m)$．这种坐标系已由 D. Hilbert (1899)給出，但这里大致上模仿了 M. Hall (1943)。

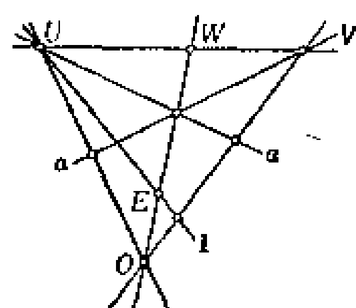


图　6.1

作为坐标的元素集合記为 $\mathfrak{C}$．在§4的例子中，$\mathfrak{C}$ 由0和1組成。一般，允許重复，記集合 $\mathfrak{C}$ 的任意三个元素为 $x$, $m$, $b$．令 $P$ 为直綫 $(0, b)\cup(m)$ 和通过 $U$ 的直綫 $x$ 的交点，并記連結 $P$ 和 $V$ 的直綫号碼为 $y$，則

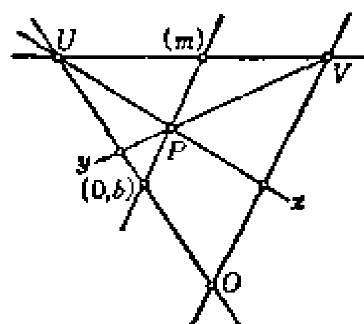


图　6.2

$$y \stackrel{d}{=} T(x, m, b) \tag{6.4}$$

唯一决定。从定义推出，对 $\mathfrak{C}$ 的任意元素 $a$, $c$, $m$, …,

(1) $T(0, m, c)=T(a, 0, c)=c$; (6.5)

(2) $T(1, m, 0)=T(m, 1, 0)=m$; (6.6)

(3) 唯一存在 $z$ 使

$$T(a, m, z)=c; \tag{6.7}$$

(4) 若 $m_1 \neq m_2$,则唯一存在 $x$ 使

$$T(x_1, m_1, b_1)=T(x, m_2, b_2); \tag{6.8}$$

(5) 若 $a_1 \neq a_2$,则唯一存在一对 $m$, $b$ 使

$$T(a_1, m, b)=c_1, \quad T(a_2, m, b)=c_2. \tag{6.9}$$

满足上列(1)～(5)的 $\mathfrak{C}$, 叫做**三分量系**。按上述方法在平面 $\pi$ 上构成的三分量系,叫做該**平面的三分量系**。对任意三分量系,有下列性质:

(6) 若 $m \neq 0$, 則唯一存在 $x$ 使

$$T(x, m, b)=c; \tag{6.10}$$

(7) 若 $a \neq 0$, 則式

$$T(a, y, b)=c \tag{6.11}$$

对唯一的 $y$ 成立。

(6)的証明是簡单的。从(4)推出,当 $m \neq 0$ 时存在唯一 $x$ 使

$$T(x, m, b)=T(x, 0, c). \tag{6.12}$$

由(1),上式右边等于 $c$. 因此,这个 $x$ 就是(6)中的 $x$.

(7)的証明。令 $a \neq 0$, 則由(5)推出,

$$T(a, y, z)=c, \quad T(0, y, z)=b \tag{6.13}$$

的解 $y$, $z$ 唯一存在。由(1), $z=b$. 而由(3), 解 $b$ 唯一决定。因此,这个 $y$ 就是欲求的唯一解。

反之, 令 $\mathfrak{C}$ 为一个三分量系, 并令 $a$, $b$, $c$, $m$, … 为它的元素, $A$, $l_\infty$ 为某些輔助記号,則存在 $PG$ 具有点$(a, c)$, $(m)$, $A$ 以及直綫

$$y=T(x, m, b), \quad x=a, \quad l_\infty, \tag{6.14}$$

而且它們之間的結合关系如下:

(i) 当且仅当

$$c=T(a,\ m,\ b) \tag{6.15}$$

时，$(a,\ c)$ 同 $y=T(x,\ m,\ b)$ 結合；

(ii) 对任意的 $c$，$(a,\ c)$ 同 $x=a$ 結合；

(iii) 对任意的 $b$，$(m)$ 同 $y=T(x,\ m,\ b)$ 結合；

(iv) 对所有的 $m$，$(m)$ 同 $l_\infty$ 結合；

(v) $A$ 同 $l_\infty$ 以及对所有的 $a$，同 $x=a$ 結合。

这些条件給出一个具有 $A=U$，$(0)=V$，$(0,0)=O$，$(1,1)=E$ 和 $l_\infty=UV$ 的平面三分量系。

关于三分量系的 $T(a,\ m,\ b)$ 的构造，詳細情形仍未得到。特别当 $\mathfrak{C}$ 为实数体时，

$$T(a,\ m,\ b)=am+b \tag{6.16}$$

具有上列性质。从这个事实反过来考虑，对号碼 $0,\ 1,\ a,\ b,\cdots$，用

$$T(a,\ 1,\ b)\overset{\mathrm{d}}{=}a+b, \tag{6.17}$$

$$T(a,\ b,\ 0)\overset{\mathrm{d}}{=}ab \tag{6.18}$$

定义加法和乘法，而把遵循这个定义的加法和乘法的 $\mathfrak{C}$ 叫做**平面的自然区域**。一般，自然区域不决定生成它的三分量系，所以也把 (6.17) 和 (6.18) 分别称为**第一**和**第二可分解条件**。在自然区域中，从作图法显然看出

(I) $a\cdot 1=1\cdot a=a$，（单位元素的存在性） (6.19)

(II) $a+0=0+a=a$，（零元素的存在性） (6.20)

(III) $a\cdot 0=0\cdot a=0$。 (6.21)

由此可知号碼 0 相当于加法中的中性元素，即**零元素**，号碼 1 相当于乘法中的中性元素，即**单位元素**。从 (3) 推出，

(IV) 唯一存在 $x$ 使

$$a+x=c \quad （减法的唯一性）。 \tag{6.22}$$

由(6)和(7)推出，唯一存在 $x$ 和 $y$ 分别使

$$\text{(V)}\quad xb=c \quad (b\neq 0), \tag{6.23}$$

（除法的唯一性）

$$\text{(VI)}\quad ay=c \quad (a\neq 0). \tag{6.24}$$

使三分量系一般化的方法，是改变通过 $U, V, O$ 的綫束号碼的記号法，而不改变同一綫束中对不同直綫給予不同号碼的記号法，以及不改变不同綫束的直綫之間的一一对应。例如，通过 $O$ 和 $(a, a)$ 的直綫，不記作 $(a)$ 而記作 $f(a)$，此处規定 $f(0)=0$，幷設

$$a+b\overset{\mathrm{d}}{=}T(a, f(a), b) \tag{6.25}$$

(Л. А. Скорняков, 1949)。这样一来，在一个平面上可以构造各种各样的三分量系，但它們不一定是代数上的同构。但是它們幷不相互独立，在它們之間成立着某种代数关系。要使同一平面上的一个三分量系变到另一个三分量系，只須把下列四种变换組合起来卽可。

(a) **顯同位** 更换綫束号碼。固定三分量系的非零元素 $e, u$，幷定出 $\xi, \eta$ 使

$$e(a\xi)=a, \quad (b\eta)u=b. \tag{6.26}$$

新的三分量系是

$$T_w(a, m, b)\overset{\mathrm{d}}{=}T(a, (mu)\xi, bu)\eta. \tag{6.27}$$

这时 $e$ 是新系的单位元素。

(b) **第一类逆轉** 改变两点 $U$ 和 $V$ 的作用。

(c) **第二类逆轉** 改变两点 $V$ 和 $O$ 的作用。

(d) **移动** 沿 $UO$ 使点 $O$ 移动。固定 $s$，則当

$$y+s=T(a, m, b+s) \tag{6.28}$$

时，再設

$$y\overset{\mathrm{d}}{=}T_t(a, m, b). \tag{6.29}$$

一般，这样一来单位元素就不存在。

## §7　平面上的构形❶

最簡单例子之一，是§4中例1的构形 $7_3$, 这就是以处于平面上任意一般位置的四点 0, 1, 2, 5 为生成系而主張 $01\cup 25=3$, $12\cup 05=4$, $20\cup 15=6$ 在同一直綫上的构形定理。这在任意的 $PG$ 上不实現。

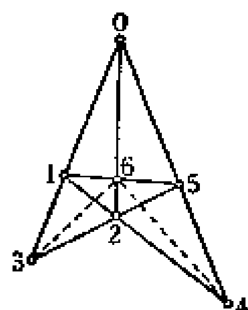



图　7.1

設 $U=0$, $V=2$, $O=1$, 又令 $E$ 在 16 上。設 04 的号碼为 $a$, 則 23 的号碼也为 $a$, 因而 $3=(0,a)$. 因为 $6=(1)$, 所以从 (6.4) 的定义推出，36 的方程是

$$y=T(x, 1, a). \tag{7.1}$$

从(6.17)推出，在这个平面的自然区域上，

$$y=x+a. \tag{7.2}$$

因为 $4=(a, 0)$ 在这个区域上，所以

$$0=a+a. \tag{7.3}$$

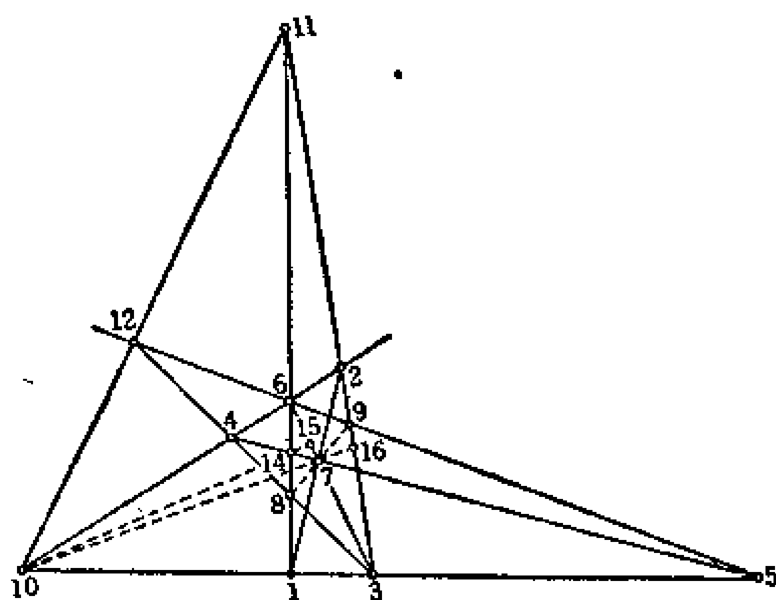



图　7.2

❶ M. Hall, Jr.: The Theory of Groups (MacMillan, New York, 1959)对射影平面有精采的叙述。——譯者注

反之,若(7.3)成立,则3, 4, 6在同一直綫上。由此可知,构形$7_3$在其自然区域全体上,当且仅当$PG$对任意的$a$满足(7.3)时成立。在§4的例1中,設$1+1=2=0$就是这个原因。

其次,当5在$1\cup3$上时,令1, 2, 3, 4, 5为生成系,则

$$\left.\begin{matrix}1&2\\4&5\end{matrix}\right\}7\quad\left.\begin{matrix}3&7\\2&4\end{matrix}\right\}6\quad\left.\begin{matrix}3&4\\1&6\end{matrix}\right\}8\quad\left.\begin{matrix}2&3\\5&6\end{matrix}\right\}9\quad\Big|7,8,9$$

叫做**Pappus第一小定理**。若构形$7_3$成立,则Pappus第一小定理成立。利用輔助点

$$\left.\begin{matrix}1&3\\2&4\end{matrix}\right\}10\quad\left.\begin{matrix}1&6\\2&3\end{matrix}\right\}11\quad\left.\begin{matrix}3&4\\5&6\end{matrix}\right\}12,$$

并应用构形定理$7_3$于四点形3 4 5 6,四点形1 6 2 3及四点形6 7 9 11,便有

$$\left.\begin{matrix}3&4\\5&5\end{matrix}\right\}12\quad\left.\begin{matrix}4&5\\3&6\end{matrix}\right\}7\quad\left.\begin{matrix}5&3\\4&6\end{matrix}\right\}10\quad\Big|12,7,10,$$

$$\left.\begin{matrix}1&6\\2&3\end{matrix}\right\}11\quad\left.\begin{matrix}1&2\\6&3\end{matrix}\right\}7\quad\left.\begin{matrix}2&6\\1&3\end{matrix}\right\}10\quad\Big|11,7,10,$$

$$\left.\begin{matrix}6&7\\9&11\end{matrix}\right\}3\quad\left.\begin{matrix}6&9\\7&11\end{matrix}\right\}12\quad\left.\begin{matrix}7&9\\6&11\end{matrix}\right\}13\quad\Big|3,12,13.$$

因为$3\cup12$与$6\cup11$只交于8,所以13与8一致。(証毕)

Pappus第一小定理成立的平面的自然区域关于加法形成**可換群**。为了証明这一点,首先設$1=(0, b)$, $2=(b, b)$, $3=U$, $4=(a, a)$, $5=(0, a)$. 于是

$$\left.\begin{matrix}1\cup2 & y=b\\4\cup5 & y=a\end{matrix}\right\}7=V\qquad\left.\begin{matrix}3\cup7 & l_\infty\\2\cup4 & y=x\end{matrix}\right\}6=(1),$$

$$\left.\begin{matrix}3\cup4 & x=a\\1\cup6 & y=x+b\end{matrix}\right\}8=(a,\ a+b)\qquad\left.\begin{matrix}2\cup3 & x=b\\5\cup6 & y=x+a\end{matrix}\right\}9=(b, b+a).$$

故8, 9和$7=V$在同一直綫上,所以

(VII) $a+b=b+a$ (加法可換律) (7.4)

成立。因为(6.20)和(6.22)已經成立，所以只須証明加法結合律成立即可。設 $1=(0, a+b)$, $2=(a, a+b)$, $3=U$, $4=(c, c+b)$, $5=(0, c+b)$, 則

$$\left.\begin{matrix} 1\cup 2 & y=a+b \\ 4\cup 5 & y=c+b \end{matrix}\right\}7=V \qquad \left.\begin{matrix} 3\cup 7 & l_\infty \\ 2\cup 4 & y=x+b \end{matrix}\right\}6=(1),$$

$$\left.\begin{matrix} 3\cup 4 & y=c \\ 1\cup 6 & y=x+(a+b) \end{matrix}\right\}8=(c, c+(a+b)),$$

$$\left.\begin{matrix} 2\cup 3 & x=a \\ 5\cup 6 & y=x+(c+b) \end{matrix}\right\}9=(a, a+(c+b)).$$

因为通过 $V$ 的直綫号碼为一定，所以

$$c+(a+b)=a+(c+b). \tag{7.5}$$

对上式两边应用(7.4)，便得

(VIII) $(a+b)+c=a+(b+c)$ (加法結合律)。(7.6) (証毕)

因此，特別是构形 $7_3$ 成立的平面上的任意自然区域，关于加法形成可換群。与 Pappus 第一小定理对偶的定理叫做 **Pappus 第二小定理**。

作为§5中 Desargues 定理的特殊情形，若一个三角形的三个頂点分別在另一个三角形的三边上时，分別把它們叫做构形定理 $D_{10}$, $D_9$, $D_8$, 此处足碼是构形的秩。$D_{10}$ 叫做 **Desargues 小定理**。若构形定理 $7_3$ 在平面上的任何部分都不成立，則 $D_9$ 蘊涵 $D_{10}$。 $D_8$ 当且仅当处于一般位置的任意四点生成后面即将提到的 Pappus 部分平面时才成立 (Miss R. Moufang, 1931)。$D_8$ 不蘊涵 $D_9$, 但 $7_3$ 蘊涵 $D_9$。

給平面射影几何 $PG[2, t]$ 的一直綫以特殊作用，并称之为无限远直綫。在除掉这条直綫和它上的所有点以后的平面几何，叫做**平面仿射几何**，并記为 $EG[2, t]$ (参見§9)。作为公理系，我們有

$EG_2.1$ (与§4中的$PG_2.1$相同)

$EG_2.2$ 必存在而且只存在一条直綫 $b$ 結合着不在直綫 $a$ 上的一点 $A$,并与 $a$ 沒有公共之点。$a$, $b$ 称为平行的。

$EG_2.3$ 至少有三点不結合着同一直綫。

滿足这些公理系的点集以及作为它的子集的直綫的全体就是 $EG[2, t]$. 构形定理要求部分平面上的点有二个或者二个以上在这条特殊直綫上。

1) **Veblen-Wedderburn 平面**❶(略記为 **V-W 平面**) 以平面上的无限远直綫 $l_\infty$ 为透視軸,并且 Desargues 小定理仿射地成立的平面,叫做 V-W 平面。在这个平面的任意自然区域的坐标集合 $\mathfrak{C}$ 上,成立着§6的(I)～(VI)以及§7的(VII)和(VIII),此外还有

(IX) $(a+b)c=ac+bc$ (左側分配律). (7.7)

(X) 对任意的 $r$, $s$, $b$,当 $r\neq s$ 时唯一存在 $x$ 使

$$xr=xs+b. \tag{7.8}$$

具有性质(I)～(X)的自然区域,叫做 **Veblen-Wedderburn 区域**。在 V-W 平面上 Pappus 第一小定理仿射地成立。在图 7.2 中,取

$$\left.\begin{matrix}1 & 6\\ 4 & 5\end{matrix}\right\}14 \quad \left.\begin{matrix}3 & 6\\ 10 & 14\end{matrix}\right\}15 \quad \left.\begin{matrix}7 & 10\\ 2 & 3\end{matrix}\right\}16,$$

并应用 $D_{10}$ 于 △2 4 16 和 △1 14 10, 則 $15'\overset{d}{=}4\ 16\cap 10\ 14$, 3 和 6 在同一直綫上, 因而 $15'=15$. 因此, 4, 15, 16 在同一直綫上。应用 $D_{10}$ 的逆定理于 △10 2 16 和 △14 8 4, 則 15 是透視中心, 因而 2,8 和 15 在同一直綫上。最后,再应用 $D_{10}$ 于 △5 10 14 和 △9 2 8,則 3, 7 和 15 在通过透視中心 6 的直綫上(証毕)。由此推出,此区域关于加法形成一个可換群。

❶ Veblen-Wedderburn[62].——譯者注

在图 7.3 中，設 $4=U$, $7=V$, $1'=O$, $2'=(a,\ am)$, $1=(0,b)$, $6=(1)$，并以这些作为生成系。由此推出 $5=(m)$, $3'=(am,am)$，又从 (6.12)，$1\cup 6$ 是 $y=x+b$. $1\cup 5$ 是 $y=T(x,\ m,\ b)$. 故 $2=(a,\ T(a,\ m,\ b))$. 因为 2, 3 和 7 在同一直綫上，所以

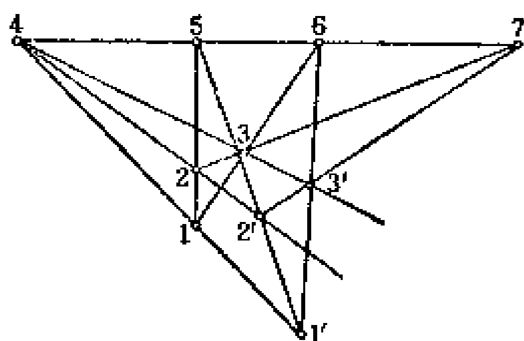



图 7.3

$$T(a,\ m,\ b)=am+b. \quad (7.9)$$

因此从 (6.8) 和 (7.9) 推出，唯一存在 $x$ 使

$$xr=T(x,\ r,\ 0)=T(x,\ s,\ b)=xs+b. \quad (7.10)$$

这就是 (X). 为了証明剩下的 (IX)，在图 7.3 中設 $7=U$, $4=V$, $1'=O$, $3'=(a,\ a)$, $5=(m)$, $1=(b,\ 0)$，并以这些作为生成系。$6=(1)$.

$$\left.\begin{matrix}1\cup 6 & y=x-b\\ 3\cup 4 & y=a\end{matrix}\right\}3=(a+b,\ a) \qquad \left.\begin{matrix}1'\cup 5 & y=xm\\ 3'\cup 7 & x=a\end{matrix}\right\}2'=(a,\ am),$$

$$\left.\begin{matrix}2'\cup 4 & y=am\\ 3\cup 7 & x=a+b\end{matrix}\right\}2=(a+b,\ am).$$

从 (7.9)，$1\cup 5$ 是 $y=xm-bm$. 因为 2 在 $1\cup 5$ 上，所以

$$am=(a+b)m-bm. \quad (7.11)$$

利用 $\mathfrak{C}$ 关于加法形成群这个事实便得出 (IX). 根据特殊直綫上的 $U$, $V$ 的选擇，可得到不同的自然区域，但是它們不一定为同构。

反之，具有性质 (I) ~ (X) 的三分量系使在 (7.9) 所定义的区域上构成满足 §6 中 (i) ~ (v) 的平面，就是 V-W 平面。与 V-W 平面对偶的平面未必为 V-W 平面，但是 (I) ~ (VIII) 成立，而代替 (IX) 和 (X) 成立着下列的

(IX′) $a(b+c)=ab+ac$ （右側分配律）， (7.12)

(X′) 对任意的 $r$, $s$, $b$，当 $r\neq s$ 时唯一存在 $x$ 使

$$rx = sx + b. \tag{7.13}$$

V-W 平面的 $\mathfrak{C}$ 叫做**左侧拟域**，而与此对偶的平面的 $\mathfrak{C}$ 叫做**右侧拟域**。

2) **交代平面** Desargues 小定理成立的平面叫做交代平面或者 **Moufang 平面**。在这个平面的自然区域中，除(I)～(X)和(IX')之外，还成立着

(XI) $[a, a, b]=0$ （左侧重合律）, (7.14)

(XII) $[b, a, a]=0$ （右侧重合律）. (7.15)

这里**結合积**由次式定义:

$$[a, b, c] \overset{\text{d}}{=} (ab)c - a(bc). \tag{7.16}$$

这时称 $\mathfrak{C}$ 为**交代域**。反之，利用直射变换可以証明，交代域上构成的平面是交代平面。与交代平面对偶的平面也是交代平面。这可从 Desargues 小定理是自对偶这个事实推出。但是，交代平面本身不一定是自对偶的。

在交代平面上的至少一个自然区域中，当且仅当

(XIII) $[a, b, c]=0$ （乘法結合律） (7.17)

时，Desargues 定理成立。

3) **Desargues 平面**（略記为 **D 平面**） Desargues 定理射影地成立的平面叫做 D 平面。在 D 平面上成立着乘法結合律。这时称 $\mathfrak{C}$ 为**斜域**❶。反之，具有斜域为自然区域的平面是 D 平面。因为在三維或者三維以上的 $PG$ 中 Desargues 定理必成立，所以 D 平面是可以嵌入三維或者三維以上的 $PG$ 内的唯一平面。

4) **Pappus 平面**（略記为 **P 平面**） 三点 1, 3, 5 和三点 2, 4, 6 分别在同一直綫上，并且

$$\left.\begin{matrix}1 & 2\\ 4 & 5\end{matrix}\right\}7 \quad \left.\begin{matrix}2 & 3\\ 5 & 6\end{matrix}\right\}9 \quad \left.\begin{matrix}3 & 4\\ 6 & 1\end{matrix}\right\}8 \quad \Big| 7, 8, 9$$

❶ 也称为除环 (sfield)。——譯者注

成立时，这叫做 **Pappus 定理**。在这个平面上的所有自然区域中，当且仅当

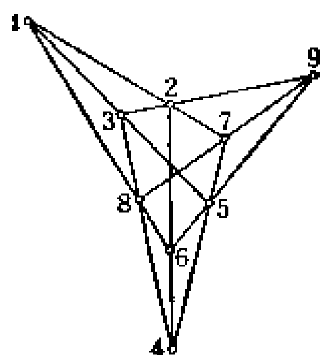


图 7.4

(XIV) $[a, b]=0$ （乘法可换律） (7.18)

时，Pappus 定理射影地成立。Pappus 定理射影地成立的平面叫做 P 平面。这里**交换积**由次式定义：

$$[a, b]\stackrel{d}{=}ab-ba. \qquad (7.19)$$

这时称 $\mathfrak{C}$ 为域。反之，在域上构成的平面是 P 平面。

在上面我們不假定在平面上的不同点的个数是有限的。若平面上的点的个数为有限，則 $\mathfrak{C}$ 中不同元素个数即阶也为有限。阶 $t$ 为有限的域，叫做 **Galois 域**，記作 $GF[t]$. $GF[t]$ 当 $t$ 为素数或者素数幂时必存在，而对其他的 $t$ 就不存在❶。Galois 域的构造，除掉同构以外，仅由 $t$ 决定，所以有限 D 平面，除掉同构的以外，仅由它上的点的个数决定。阶为有限的斜域都是 Galois 域❷。因此，在有限射影平面中就沒有 D 平面与 P 平面的区别。又因阶为有限的交代域都是 Galois 域，所以在有限射影平面中也沒有交代平面与 P 平面的区别。但是在有限射影平面中却存在着不是 D 平面的 V-W 平面 (O. Veblen, J. M. Maclagan-Wedderburn, 1907)。在 $PG[2,t]$ 中当 $t=2, 3, 4, 5$ 时 V-W 平面与 D 平面一致，但当 $t=6$ 时，如 §15 所述，$PG$ 不存在。当 $t=7$ 时，利用边长为 7 的拉丁方可以驗証在 $PG$ 中只存在 D 平面。当 $t=8$ 时，利用 $GF[2^3]$ 可以构造 D 平面，但是，不是 D 平面的 $PG$ 存在与否，长时期以来一直沒有解决。到了 1956 年，利用穿孔卡进行机械計算

---

❶ 參看附录。

❷ 正田健次郎：抽象代数学，岩波，1932，第4章 §18, Levi [5], Pickert [9], Artin [12].

才确认只存在D平面。

当$t=9$时，更改乘法表❶，可以由$GF[3^2]$构造不是D平面的V-W平面。这在代数方面的思想应归功于L. E. Dickson❷(1905)。取$a+bj\ (j^2=-1)$为$\mathfrak{C}$的元素，并令$a, b$为$GF[3]$的元素0, 1, 2中的任一个。規定加法与$GF[3^2]$的元素的情形相同。設$\mathfrak{C}$的任意两个元素$x, y$的乘法$x\circ y$等于$GF[3^2]$的元素的$xy$或者$xy^3$，并根据$x$为$GF[3^2]$中某个元素的平方或否而取前者或后者。亦即設

$$x\circ y=\begin{cases}xy, & x\text{为平方剩余},\\ xy^3, & x\text{为平方非剩余}。\end{cases} \tag{7 20}$$

对于左因子，分配律成立，但对于右因子，分配律就不成立。显然，这与$GF[3^2]$是不同构的。要証明$\mathfrak{C}$为左側拟域，是容易的。特别，因为乘法結合律成立的右側(或者左側)拟域的研究可以归結为二重傳递群的研究，所以研究后者的构造是有益的❸。例如，当阶$t$为有限的情形，可以推出$t$只能是素数或者素数幂。

与上述来自点代数观点的研究相反，R. Baer (1940)从直射变换和对射变换的观点描述了各种平面的特征。設与点$P$在同一直綫上但不同于$P$的任意两点$A, A'$不在直綫$g$上。若使$A$变为$A'$的直射变换保持$g$上所有的点以及通过$P$的所有直綫不变，则称这个平面为$(P, g)$傳递。又当$P$不在$g$上时，設存在既不在$g$上又不同于点$P$的任意一点$A$，以及通过$AP\cap g\overset{\mathrm{d}}{=}Z$而不通过$P$的任意直綫$h$，使得$h$与$g$相交，但$g\neq h$。若有对射变换使$A$变为$h$，$g$上的点$X$变为直綫$PX$，以及通过$P$的任意直綫$x$变为点

❶ 关于乘法表，見例如森口繁一：統計分析，刘璋溫譯，p. 68，本丛书。——譯者注

❷ L. E. Dickson: Linear Algebra, Cambridge Tracts, London, 1930, §60.

❸ H. Zassenhaus: Abh. math. Seminar Univ. Hamburg, 11 (1936), 187~220.

$x \cap g$，則称这个平面为**$(P, g)$对偶**。若固定$P$和$g$，則$(P, g)$直射变换全体形成一个群。两个$(P, g)$对射变换的乘积給出一个直射变换，反之，一个$(P, g)$直射变换可以分解为两个$(P, g)$对射变换的乘积。若給定一点的映象，則确定任意的$(P, g)$直射变换或者$(P, g)$对射变换。图 7.5 表示求$B$的映象$B'$的方法。若$B$在$AA'$上，則先求出不在$AA'$上的点$C$的映象$C'$，然后利用它便可确定$B$的映象$B'$。图 7.6 表示$B$不在$AP$上时求它的映象$l$的方法。若$B$在$AP$上，則先求出不在$AP$上的一点$D$的映象作为輔助映象卽可。

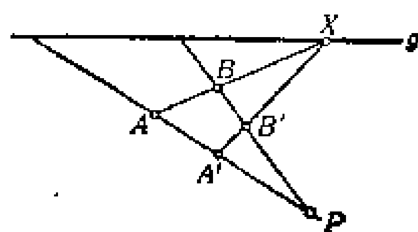



图 7.5

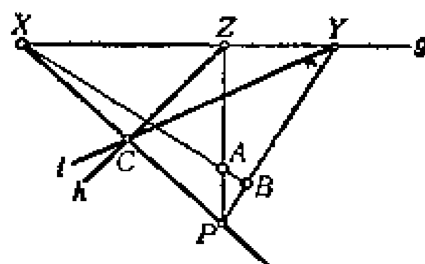



图 7.6

若平面为$(P, g)$对偶，則这个平面为$(P, g)$傳递。若平面关于直綫$h$上的任意一点$P$为$(P, g)$傳递，則称这个平面为**$(h, g)$傳递**。这样，一个平面为$(g, g)$傳递，当且仅当这个平面是 V-W 平面并且$g$是无限远直綫$l_\infty$的情形。这可以这样推出：在$l_\infty$上的任意一点$U$考虑$(U, l_\infty)$直射变换，若这是$(g, g)$傳递，則依$g$得到 Desargues 小定理。若平面为$(g, g)$傳递，并对不在$g$上的一点$P$为$(P, g)$傳递，則这个平面是 D 平面。反之，D 平面关于任意一点$P$和任意直綫$g$为$(P, g)$傳递。若平面为$(g, g)$傳递，并对不在$g$上的一点$P$为$(P, g)$对偶，則这个平面是 P 平面。反之，P 平面为$(g, g)$傳递，并对不在$g$上的任意一点$P$为$(P, g)$对偶。这种做法未能描述交代平面的特征。

令$\Phi$为平面上的一个直射变换。若由$\Phi$生成的循环群，关于

这个平面上的所有点为傳递，則称这个平面为**循环平面**。循环平面上的点或者直綫的个数至多是可数的。若 $\Phi$ 的阶为有限，则循环平面是有限射影平面，对 BIB 的构造能起作用的就是这种場合。所有有限的 D 平面都是循环的。若循环平面关于一直綫 $g$ 以及它上的一点 $P$ 为 $(P, g)$ 傳遞，则这个平面是 D 平面。仍未得到有限平面中不是 D 平面的循环平面❶。人們猜想这种平面恐怕不会存在。

## §8 Galois 域上的射影几何

从上节我們已經看到，在有限射影平面中 Desargues 定理成立的情形，坐标集合 $\mathfrak{G}$ 只能是 $GF[t]$. 根据 §5，对有限的 $PG$，当 $s \geqslant 3$, $t \geqslant 2$ 时 Desargues 定理必成立，所以具有 $s \geqslant 3$, $t \geqslant 2$ 的 $PG[s, t]$ 可从 Galois 域来构造，或者只能是与此同构的。因此，$t$ 必須是素数或者素数幂。

把 $GF[t]$ 中 $s+1$ 个不全为 0 的元素排成

$$A \stackrel{\mathrm{d}}{=} [a_1, a_2, \cdots, a_{s+1}], \tag{8.1}$$

并称为点 $A$，而 $a_i$ 称为第 $i$ 个坐标。令 $\rho$ 为 $GF[t]$ 中非零的任意元素，如 §4 的例 1 那样，規定

$$\rho A \stackrel{\mathrm{d}}{=} [\rho a_1, \rho a_2, \cdots, \rho a_{s+1}] \tag{8.2}$$

与 $A$ 表示同一点。使 $A$ 的所有坐标变动，则得到 $t^{s+1}$ 个点。按規定，要除去坐标全为零的点，所以只剩下 $(t^{s+1}-1)$ 个点。根据 (8.2)，其中每一点分别有 $t-1$ 个相同点，于是不同点的个数是

$$v = (t^{s+1}-1)/(t-1) = t^s + t^{s-1} + \cdots + t + 1. \tag{8.3}$$

設

$$\phi(s, d, t) \stackrel{\mathrm{d}}{=} \frac{(t^{s+1}-1)(t^s-1)\cdots(t^{s-d+1}-1)}{(t^{d+1}-1)(t^d-1)\cdots(t-1)}, \tag{8.4}$$

❶ 在无限平面中存在着不是 D 平面的循环平面。

則由定义有

$$\phi(s, d, t)=\phi(s, s-d-1, t). \tag{8.5}$$

于是作为 $\phi$ 的函数給出的量，当固定 $s, t$ 时，变换 $d$ 与 $s-d-1$ 仍然不变。这相应于§4的对偶原理。按此記号記作

$$v=\phi(s, 0, t). \tag{8.6}$$

从(8.3)容易看出，若 $t\geqslant 2$，則至少存在三个不同点。令 $A, B$ 为不同的两点，$\mu, \nu$ 为 $GF[t]$ 中不同时为0的元素，則点

$$\mu A+\nu B\overset{\text{d}}{=}[\mu a_1+\nu b_1, \mu a_2+\nu b_2, \cdots, \mu a_{s+1}+\nu b_{s+1}] \tag{8.7}$$

全体叫做結合 $A, B$ 的直綫。当固定 $A, B$ 时，这条直綫上的点表为 $\{\mu, \nu\}$。令 $\rho$ 为 $GF[t]$ 中非零元素，則

$$\rho\{\mu, \nu\}\overset{\text{d}}{=}\{\rho\mu, \rho\nu\} \tag{8.8}$$

与(8.7)表示相同的点。因此，按照前面的論証，可知这条直綫上有

$$k_1=\phi(1, 0, t)=t+1 \tag{8.9}$$

个不同点。若 $k\geqslant 2$，則

$$\phi(k, 0, t)>\phi(1, 0, t), \tag{8.10}$$

所以存在点 $C$ 不在这条直綫上。称 $A, B, C$ 为**綫性独立**。令 $\lambda, \mu, \nu$ 为 $GF[t]$ 中不全为0的元素，則点

$$\lambda A+\mu B+\nu C\overset{\text{d}}{=}[\lambda a_1+\mu b_1+\nu c_1, \cdots, \lambda a_{s+1}+\mu b_{s+1}+\nu c_{s+1}] \tag{8.11}$$

全体叫做結合 $A, B, C$ 的平面。当固定 $A, B, C$ 时，这个平面上的点表为 $\{\lambda, \mu, \nu\}$。令 $\rho$ 为 $GF[t]$ 中非零元素，并規定

$$\rho\{\lambda, \mu, \nu\}\overset{\text{d}}{=}\{\rho\lambda, \rho\mu, \rho\nu\}, \tag{8.12}$$

則按照前面的論証，便有

$$k_2=\phi(2, 0, t)=t^2+t+1. \tag{8.13}$$

令 $D$ 为不在这个平面上的点，則称 $A, B, C, D$ 为綫性独立。

令点为零維空間，直綫为一維空間，平面为二維空間。那末，設 $0\leqslant d\leqslant s$，并令 $\lambda_1, \lambda_2, \cdots, \lambda_{d+1}$ 为 $GF[t]$ 中不全为 0 的元素，則一般的 $d$ 維空間可以定义为

$$\lambda_1 A_1+\lambda_2 A_2+\cdots+\lambda_{d+1}A_{d+1}\overset{\mathrm{d}}{=}[b_1, b_2, \cdots, b_{s+1}] \quad (8.14)$$

的全体，此处令 $a_{\alpha i}$ 为 $GF[t]$ 中不全为 0 的元素，并設

$$b_i\overset{\mathrm{d}}{=}\lambda_1 a_{1i}+\lambda_2 a_{2i}+\cdots+\lambda_{d+1}a_{d+1,i}. \quad (8.15)$$

若对任意的 $i$，上式右边当 $\lambda_1, \lambda_2, \cdots, \lambda_{d+1}$ 全为 0 时才为 0，則称 $A_1, A_2, \cdots, A_{d+1}$ 为綫性独立。

(8.14) 的全体也称为 $A_1, A_2, \cdots, A_{d+1}$ 張成的空間。显然，这个点集满足 $PG.1$. 对 $\rho\neq 0$，以及不同的两点 $A, B$，若

$$\mu A+\nu B=\mu' A+\nu' B,\ \{\mu, \nu\}\neq\rho\{\mu', \nu'\}, \quad (8.16)$$

則

$$(\mu-\mu')A+(\nu-\nu')B=0. \quad (8.17)$$

因为 $A, B$ 为綫性独立，所以 $\mu=\mu'$, $\nu=\nu'$. 这与假定矛盾。因此 $PG.2$ 也成立。对綫性独立的三点 $A, B, C$，設

$$\left.\begin{aligned} D&\overset{\mathrm{d}}{=}\mu_1 A+\nu_1 B,\ \mu_1\nu_1\neq 0,\\ E&\overset{\mathrm{d}}{=}\mu_2 B+\nu_2 C,\ \mu_2\nu_2\neq 0,\end{aligned}\right\} \quad (8.18)$$

則

$$\mu_2 D+(-\nu_1)E=\mu_1\mu_2 A+(-\nu_1\nu_2)C\overset{\mathrm{d}}{=}F. \quad (8.19)$$

这表示直綫 $DE$ 和直綫 $AC$ 的交点 $F$ 的存在性，所以 $PG.3$ 也成立。从构造方法不难看出，$PG.4$ 及 $PG.5$ 也成立。因此得到的就是 $PG[d, t]$. 特别，由这个方法构成的 $PG[2, t]$，因为以域为自然区域，所以是 P 平面，而因那是有限射影平面，所以也是 D 平面。

在以一般斜域为基础的 D 平面中，乘法的可換律不一定成立。因此，例如三維空間的点可用不全为 0 的元素 $x_i$ 表为

$$[x]\sigma \stackrel{d}{=} [x_1, x_2, x_3, x_4]\sigma \quad (\sigma \neq 0), \tag{8.20}$$

而平面可用不全为 0 的元素 $u_i$ 表为

$$\rho\{u\} \stackrel{d}{=} \rho\{u_1, u_2, u_3, u_4\} \quad (\rho \neq 0). \tag{8.21}$$

两者的結合表为

$$\{u\}[x] \stackrel{d}{=} u_1x_1 + u_2x_2 + u_3x_3 + u_4x_4 = 0. \tag{8.22}$$

若不同两点 $[x]$, $[y]$ 存在于不同两平面 $\{u\}$, $\{v\}$ 上，則

$$\{u\}[x] = 0, \ \{v\}[x] = 0, \ \{u\}[y] = 0, \ \{v\}[y] = 0 \tag{8.23}$$

同时成立，并且分配律成立，故可以推出，点束 $[x\lambda + y\mu]$ 在面束 $\{\sigma u + \tau v\}$ 上，此处点束乃是綫束的对偶概念。这个点束或者面束表示一直綫。这里，若特别考虑两个平面

$$\rho\{u_1, u_2, u_3, 0\}, \quad \rho\{0, 0, 0, 1\} \tag{8.24}$$

的交綫，則

$$u_1x_1 + u_2x_2 + u_3x_3 = 0, \quad x_4 = 0. \tag{8.25}$$

(8.25) 中左边式子表示平面上的点与直綫的結合关系，因而用这个式子可使二維空間中的点与这个平面上的点一一对应，并保持結合关系不变。由此可知，D 平面可以嵌入 $PG[s, t]$ $(s \geqslant 3)$.

对于 $d$ 維空間的构造，第一点 $A_1$ 有 $\phi(s, 0, t)$ 种选擇，第二点 $A_2$ 有 $[\phi(s, 0, t) - 1]$ 种选擇，而第三点 $A_3$ 要选擇与 $A_1$, $A_2$ 綫性独立，所以要除去直綫 $A_1A_2$ 上的点，于是剩下 $[\phi(s, 0, t) - \phi(1, 0, t)]$ 种选擇，…. 故綫性独立的 $d+1$ 个点有

$$\phi(s, 0, t)[\phi(s, 0, t) - 1][\phi(s, 0, t) - \phi(1, 0, t)] \cdots [\phi(s, 0, t) - \phi(d-1, 0, t)] \stackrel{d}{=} f(s, 0, d, t) \tag{8.26}$$

种选擇。但是，在 $A_1, A_2, \cdots, A_{d+1}$ 張成的空間中，綫性独立的 $d+1$ 个点各有 $f(d, 0, d, t)$ 种选擇，所以除去这么多的重复后，$PG[s, t]$ 中的不同 $PG[d, t]$ 的个数是

$$b_d = f(s, 0, d, t) / f(d, 0, d, t) = \phi(s, d, t), \tag{8.27}$$

此处設

$$\phi(s, -1, t) \stackrel{d}{=} 1. \tag{8.28}$$

下面往求包含 $PG[d, t]$ 但被包含于 $PG[s, t]$ 中的 $PG[f, t]$ 的个数，此处 $0 \leqslant d < f \leqslant s$. 首先，不包含于 $PG[d, t]$ 中的一点 $A_{d+2}$ 有

$$\begin{aligned}\phi(s, 0, t) - \phi(d, 0, t) &= (t^{s+1} - t^{d+1}) / (t-1) \\ &= t^s + t^{s-1} + \cdots + t^{d+1}\end{aligned} \tag{8.29}$$

种选擇。$A_{d+3}$ 要从不包含 $PG[d, t]$ 和 $A_{d+2}$ 的 $PG[d+1, t]$ 的点中来选擇，所以有 $[\phi(s, 0, t) - \phi(d+1, 0, t)]$ 种选擇。继續这个程序到得到 $PG[f, t]$ 为止，则总共有

$$\begin{aligned}f(s, d, f, t) \stackrel{d}{=} &[\phi(s, 0, t) - \phi(d, 0, t)][\phi(s, 0, t) \\ &-\phi(d+1, 0, t)]\cdots[\phi(s, 0, t) - \phi(f-1, 0, t)]\end{aligned} \tag{8.30}$$

种选擇。如前面一样，各点每有 $f(f, d, f, t)$ 个重复，所以除去这些重复后，便得到欲求的个数

$$f(s, d, f, t) / f(f, d, f, t) = \phi(s-d-1, f-d-1, t). \tag{8.31}$$

特别令 $d=0$ 后再以 $d$ 代替 $f$，则包含特定一点的 $d$ 維空間的个数为

$$r_d = \phi(s-1, d-1, t). \tag{8.32}$$

令 $d=1$ 后再以 $d$ 代替 $f$，则同时包含特定不同两点的 $d$ 維空間的个数为

$$\lambda_d = \phi(s-2, d-2, t). \tag{8.33}$$

用与§3完全相同的方法，也可直接从(8.27)导出上列那些式子。

$PG[d, t]$ 内的点的个数，在(8.6)以 $d$ 代替 $s$ 后便得为

$$k_d = \phi(d, 0, t). \tag{8.34}$$

这里若把点譯成品种，$d$ 維空間譯成区組，则得到参数

$$v, k_d, b_d, r_d, \lambda_d$$

的 BIB. 特別当 $s=d+1$ 时是 SBIB. 效率因子是

$$E = (t^{s+1}-1)(t^d-1) / [(t^s-1)(t^{d+1}-1)]. \tag{8.35}$$

附表1的 $P$ 表示由这个方法得到的設計。

**例1**　在 $PG[3, 2]$ 中令 $d=2$，便得

$$v=b_2=15,\ k_2=r_2=7,\ \lambda_2=3,\ E=45/49.$$

考虑以 $A_1=[1\,0\,0\,0]$，$A_2=[0\,1\,0\,0]$，$A_3=[0\,0\,1\,0]$，$A_4=[0\,0\,0\,1]$为四頂点的四面体的面上的点便可。参看图9.1. 例如

$$A_1+A_2=[1\,1\,0\,0],\ A_2+A_3=[0\,1\,1\,0],\ A_1+A_3=[1\,0\,1\,0].$$

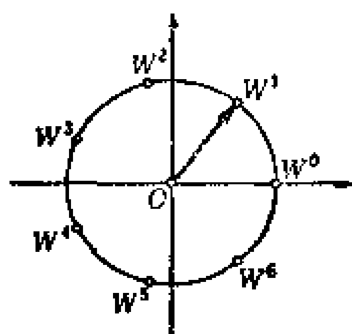



图　8.1

剩下一点是

$$[1\,0\,0\,0]+[0\,1\,1\,0]=[1\,1\,1\,0].$$

上列七点对应于同一平面亦即同一区組內的品种。取上列七点以外的一点如$[1\,0\,0\,1]$，加上在同一平面上的上列七点，便可决定包含于其他区組的七个品种。同样可以决定十五个区組。若按照§3中的組合方法去做，则需要 $b=6435$ 个(!)区組。

**例2**　利用 $PG[2, 2^3]$ 便有

$$v=b=73,\ k=r=9,\ \lambda=1,\ E=73/81.$$

首先，令 $x$ 为 $GF[p^s]$ 中非零的任意元素，则由 **Fermat 定理**，

$$x^{p^s-1}-1=0.$$

令 $p=2$, $s=3$，则

$$x^{2^3-1}-1=x^7-1=(x-1)(x^6+x^5+\cdots+x+1)=0.$$

由未定系数法，

$$x^6+x^5+\cdots+x+1=(x^3+x^2+1)(x^3+x+1).$$

上式右边各項是以 $GF[2]$ 的元素为系数的**不可約多項式**❶，也称**素函数**或者**最小函数**，亦即不能再分解为以 $GF[2]$ 的元素为系数的更低次的多項式(参看附表2)。取上式右边中的任意一項，例如

$$P_3(x)\overset{d}{=}x^3+x+1,$$

则 $P_3(x)=0$ 的一个根 $W$ 叫做**原始元素**，而若以 $P_3(x)$ 除的剩余来分类，则以 $GF[2]$ 的元素为系数的多項式都可以表为形状

❶　詳細情形，可参看 L. E. Dickson: Linear Groups with an Exposition of the Galois Field Theory (Teubner, Leipzig, 1901). Carmichael [2] 以及增山[7]，計画篇附录，都介紹了 Dickson 的方法。

$$W^i = d_2W^2 + d_1W + d_0, \quad [\mathrm{modd}\ 2,\ P_3(x)].$$

上式左边叫做 $GF[2^3]$ 的元素的**幂表現**，右边叫做 $GF[2^3]$ 的元素的**多項式表現**。把 $W^\infty$ 記作 $W^{-\infty}$ 可能容易理解，但这里 $\infty$ 只不过是記号，所以节省了負号。

表 8.1

| 幂表現 | 多項式表現 | | |
|---|---|---|---|
| $W^\infty$ | 0 | 0 | 0 |
| $W^0$ | 0 | 0 | 1 |
| $W^1$ | 0 | 1 | 0 |
| $W^2$ | 1 | 0 | 0 |
| $W^3$ | 0 | 1 | 1 |
| $W^4$ | 1 | 1 | 0 |
| $W^5$ | 1 | 1 | 1 |
| $W^6$ | 1 | 0 | 1 |
| | $d_2$ | $d_1$ | $d_0$ |

欲求例如

$$x_1 + Wx_2 + W^2x_3 = 0$$

上的点，就得先給出 $GF[2^3]$的元素 $x_2$, $x_3$，然后从上式决定 $x_1$。但必須除去同时为 0 的那些。例如令 $x_2 = W^0$, $x_3 = W^1$，則

$$x_1 = Wx_2 + W^2x_3 = W + W^3 = W^0.$$

令 $x_2 = W^0$, $x_3 = W^2$，則

$$x_1 = Wx_2 + W^2x_3 = W + W^4 = W^2.$$

这里乘法是按照幂表現，而加法是按照多項式表現进行的，并且系数和多項式已分别换上了以 2 和 $P_3(x)$ 为模的剩余。

如此决定了两点 $A \overset{\mathrm{d}}{=} [W^0, W^0, W^1]$, $B \overset{\mathrm{d}}{=} [W^2, W^0, W^1]$ 之后，令 $\mu$, $\nu$ 为 $GF[2^3]$中不同时为 0 的元素，便可决定 $\mu A + \nu B$。于是可以决定七点，再加上 $A$ 和 $B$ 便可决定同一直綫上的九点。这对应于一区組中的九个品种。其余如例 1 那样，只要把不在这条直綫上的一点加上已得到的九点即可。

## §9 Galois 域上的仿射几何

往求 $PG[s, t]$ 的点中公共于 $PG[s-1, t]$和不完全被后者包含的 $PG[f, t]$ 的个数。令 $A_1$ 为 $PG[f, t]$ 中的一点不包含于 $PG[s-1, t]$。因为 $A_1$ 和 $PG[s-1, t]$中的点 $B_1, B_2, \cdots, B_s$ 为綫性独立，所以 $PG[s, t]$ 中的点可表为形状

$$\lambda_1A_1 + \mu_1B_1 + \mu_2B_2 + \cdots + \mu_sB_s. \quad (9.1)$$

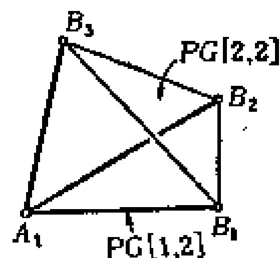


图 9.1

令 $A_1, A_2, \cdots, A_{f+1}$ 为 $PG[f, t]$中的綫性独立点，則适当地选择 $\lambda, \mu_i$ 便可把这些点表为形状 (9.1)。例如設

$$A_i=\lambda_{i1}A_1+\mu_{i1}B_1+\mu_{i2}B_2+\cdots+\mu_{is}B_s \quad (i=1,\ 2,\ \cdots,\ f+1). \tag{9.2}$$

于是

$$A_i'\overset{d}{=}A_i-\lambda_{i1}A_1 \tag{9.3}$$

仅由 $B_1, B_2, \cdots, B_s$ 来表达，从而是 $PG[s-1,t]$ 中的点。由于 $A_2'$, $A_3'$, $\cdots$, $A_{f+1}'$ 为綫性独立，所以它們張成的空間 $PG[f-1, t]$ 是 $PG[s-1, t]$ 的子空間，但它們也是 $PG[f, t]$ 中的点。除这些点以外，例如，若 $A_1'$ 包含于 $PG[s-1, t]$，并且与 $A_2'$, $A_3'$, $\cdots$, $A_{f+1}'$ 为綫性独立，則 $PG[f,t]$ 完全包含于 $PG[s-1,t]$，这与假定矛盾。这里若从 $PG[s, t]$ 除去 $PG[s-1, t]$ 中的点，則剩下的点形成 $s$ 維仿射几何 $EG[s,t]$. 包含于 $PG[s,t]$ 但不包含于 $PG[s-1, t]$ 的 $PG[f, t]$ 中的点，由于从 $PG[s, t]$ 除去 $PG[s-1, t]$，也就是从 $PG[s, t]$ 中的每一个 $PG[f, t]$ 除去 $PG[f-1, t]$，所以形成一个 $EG[f, t]$.

$EG[s, t]$ 中不同点的个数是

$$v_e=\phi(s,\ 0,\ t)-\phi(s-1,\ 0,\ t)=t^s. \tag{9.4}$$

$EG[s, t]$ 中的 $EG[d, t]$ 的个数 $(d<s)$ 是

$$b_{ed}=\phi(s,\ 0,\ t)-\phi(s,\ d-1,\ t). \tag{9.5}$$

一个 $d$ 維空間所包含点的个数是

$$k_{ed}=\phi(d,\ 0,\ t)-\phi(d-1,\ 0,\ t)=t^d. \tag{9.6}$$

包含同一点的 $EG[d, t]$ 的个数，如 (8.32) 一样，是

$$r_{ed}=\phi(s-1,\ d-1,\ t)=r_d. \tag{9.7}$$

包含特定不同两点的 $EG[d, t]$ 的个数，如 (8.33) 一样，是

$$\lambda_{ed}=\phi(s-2,\ d-2,\ t)=\lambda_d. \tag{9.8}$$

这里若把点譯成品种，$d$ 維空間譯成区組，則得到参数

$$v_e,\ k_{ed},\ b_{ed},\ r_{ed},\ \lambda_{ed}$$

的 BIB. 由这个方法得到的 BIB, 在附表 1 中記为 $E$.

**例1** 在§8的例1中，把特定一区組以及它所包含的品种从其余区組中除掉，便得到参数

$$v=8,\ k=4,\ b=14,\ r=7,\ \lambda=3,\ E=6/7$$

的BIB。这是§12中剩余法的一个例子。

## §10 循环空間

在后面作为例题引用的 T. P. Kirkman (1850) 問題[1] 的一个解法中，利用循环性从一个初始区組去导一个 BIB，以及利用§11中差集合的思想已經存在。把这个問題考虑为$PG[2, t]$的循环平面的問題，并使之与差集合联系起来，这应归功于 J. Singer (1938)[2]。

一般，$PG[s, t]$ 中的一点 $A$，可由 $GF[t]$ 中不全为0的 $s+1$ 个元素表为

$$A=[a_0, a_1, a_2, \cdots, a_s]. \tag{10.1}$$

如§8中例2那样，令 $x$ 为 $GF[t^{s+1}]$的一个原始元素，并利用关系

$$a_0+a_1x+a_2x^2+\cdots+a_sx^s=x^a \tag{10.2}$$

使(10.1)变为冪表現。若固定了最小函数，则 $A$ 与 $x^a$ 有一一对应。因此可以記$[x^a]$代替(10.1)中的 $A$。于是包含于$PG[s, t]$内的 $d$ 維空間，可由綫性独立的$(d+1)$个点$[x^{\alpha_0}]$, $[x^{\alpha_1}]$, $\cdots$, $[x^{\alpha_d}]$和$GF[t]$中不全为0的元素 $g_0, g_1, \cdots, g_d$ 表为

$$[g_0x^{\alpha_0}+g_1x^{\alpha_1}+\cdots+g_dx^{\alpha_d}]. \tag{10.3}$$

这叫做初始空間，而

$$\{\theta\}\stackrel{d}{=}[g_0x^{\alpha_0+\theta}+g_1x^{\alpha_1+\theta}+\cdots+g_dx^{\alpha_d+\theta}] \tag{10.4}$$

是从初始空間对

---

[1] W. W. R. Ball: Mathematical Recreations and Essays (Macmillan, London, 1892, 1940), 第10章; Netto的著书第11, 12章。这是属于 Steiner 三点系的一个例子。

[2] J. Singer[56]。——譯者注

$$\theta=0,\ 1,\ 2,\ \cdots,\ v-1 \tag{10.5}$$

生成的空間。不管 $\theta$ 是什么，$\{\theta\}$ 总是 $d$ 維空間。以 $x^{-\theta}$ 乘 $\{\theta\}$ 的右边便可看出这一点。从原根的性质的确有 $\{0\}=\{v\}$，而使

$$\{0\}=\{\theta\}\quad(\theta>0) \tag{10.6}$$

的最小 $\theta$ 叫做上述初始空間的循环数。以 $\theta$ 除 $v$，令 $q$ 为商，$r$ 为剩余，则

$$v=q\theta+r,\quad 0\leqslant r<\theta. \tag{10.7}$$

$$\begin{aligned}&[g_0x^{\alpha_0+v}+g_1x^{\alpha_1+v}+\cdots+g_dx^{\alpha_d+v}]\\&=[g_0x^{\alpha_0+r}+g_1x^{\alpha_1+r}+\cdots+g_dx^{\alpha_d+r}]\\&=[g_0x^{\alpha_0}+g_1x^{\alpha_1}+\cdots+g_dx^{\alpha_d}].\end{aligned} \tag{10.8}$$

故 $r$ 是一个循环数。若 $r>0$，則这与定义 $\theta$ 为最小循环数发生矛盾。因此 $r=0$。

因此，循环数 $\theta$ 必須是 $v$ 的約数。設

$$v=q\theta. \tag{10.9}$$

若只写下冪指数，則初始空間內的点是

$$\begin{array}{lllll}0 & \theta & 2\theta & \cdots & (q-1)\theta\\ c_1 & c_1+\theta & c_1+2\theta & \cdots & c_1+(q-1)\theta\\ \vdots & \vdots & \vdots & & \\ c_{\omega-1} & c_{\omega-1}+\theta & c_{\omega-1}+2\theta & \cdots & c_{\omega-1}+(q-1)\theta,\end{array} \tag{10.10}$$

此处設 $c_1$ 为不在第一行上的任意一点，$c_2$ 为不在第一、二行上的任意一点，…. 从构造方法容易看出，設 $c_0=0$，則当 $i\neq j$ 时

$$c_i-c_j\neq 0\pmod{\theta}. \tag{10.11}$$

由于初始空間內的点的个数是 $k_d=q\omega$，所以 $v$ 与 $k_d$ 不可能互素。若它們互素，則不存在小于 $v$ 的循环数 $\theta$. 对循环数为 $v$ 的情形，全空間的点由循环数 $v$ 的

$$\nu\overset{d}{=}b_d/v=\phi(s,\ d,\ t)/\phi(s,\ 0,\ t) \tag{10.12}$$

个初始空間生成。任意两点的相遇数当然等于(8.33)中的 $\lambda_d$。

特别，我們考虑 $d=1$ 的情形。設一条初始直綫为

$$[a_0x^0+a_1x^\theta]. \tag{10.13}$$

若 $[x^c]$ 在这条直綫上，则 $[x^{c+\theta}]$ 也是如此，所以这条直綫可以表为

$$[a_0x^c+a_1x^{\theta+c}]. \tag{10.14}$$

这意味着 $c$ 是 $\theta$ 的倍数。因此，这条直綫上的点用冪指数可表为

$$0,\ \theta,\ 2\theta,\ \cdots,\ t\theta. \tag{10.15}$$

我們有 $k_1=q=t+1$，$\omega=1$. 因此，(i) 若

$$\theta=v/k_1=(t^{s+1}-1)/(t^2-1) \tag{10.16}$$

不是整数，则任意初始直綫的循环数都是 $v$，并且初始直綫有

$$\nu_1=b_1/v=\phi(s,\ 1,\ t)/\phi(s,\ 0,\ t)=(t^s-1)/(t^2-1) \tag{10.17}$$

条。因为我們已取 $\mathfrak{G}$ 为 Galois 域，由此可知 $s=2$ 的情形，亦即有限的 D 平面是循环的。任意两点的相遇数是

$$\lambda_1=\phi(s,\ -1,\ t)=1. \tag{10.18}$$

(ii) 若 $\theta$ 是整数，则由 (10.13) 生成的直綫有 $\theta$ 条。而其余直綫由

$$\nu\stackrel{\mathrm{d}}{=}(b_1-\theta)/v=t(t^{s-1}-1)/(t^2-1) \tag{10.19}$$

条初始直綫依循环数 $v$ 生成。这时，两点 $[x^{c_i}]$，$[x^{c_j}]$ 当 $c_i-c_j\equiv0\pmod\theta$ 时在循环数 $\theta$ 生成的直綫上相遇一次，当 $c_i-c_j\not\equiv0\pmod\theta$ 时在循环数 $v$ 生成的直綫上相遇一次❶。对 $EG$ 也可以同样处理。决定初始空間无非就是一种标准化。

**例 1 Kirkman 問題** 每日把 $v=15$ 名女生排成 $k=3$ 列纵队率領郊游。欲使任意两人只有一次排在同一行，就需要 $r=7$ 日。試求这种排列。因为每日排成 $n=5$ 行，所以 $b=nr=35$，这是 RBIB 的一个例子。只須把 $PG[3,2]$ 中的 35 条直綫分为 7 組，使得每一組都包含不同的 15 点。令 $x$ 为 $GF[2^4]$ 的一个原根，$x^0$，$x^1$，$x^2$，…，$x^{14}$ 表示 15 点。求它們的多项式表現 (10.2)，并如 (10.1) 那样用系数来表示点。其中，第一个坐标为 0 的点表为 $[0,\ a_1,\ a_2,\ a_3]$，并使之对应于 §8 中例 2 的元素

❶ 对一般 $d$ 的情形，可參看 C. R. Rao: Proc. Nat. Inst. Sci. India, **11** (1945), 136～149; **12** (1946), 123～135. 对 $d=2$ 的情形，增山[8]有所介紹。

$$W^i = a_1 + a_2 W + a_3 W^2.$$

用变换 $W^i \to W^{i+1}$ 定义

$$W^{i+1} = b_1 + b_2 W + b_3 W^2,$$

則置换

$$P \overset{\mathrm{d}}{=} \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$$

的阶是 $2^3-1=7$。作 $P^2, P^3, \cdots, P^6$，而若这次逆顺地退回幂表現，則得循环置换$(CT)$

$$0\to1\to2\to9\to7\to12\to13\to0.$$

其次，对第一个坐标为1，其余坐标至少有一个不为0的点作同样操作，便得到

$$4\to10\to14\to11\to6\to5\to8\to4.$$

所有坐标全为0的点不动。亦即

$$3\to3.$$

于是先求第一日的排列，然后只須依在同一行的3人的号碼作循环置换即可。至于第一日的排列，考虑 $\theta=5$ 条初始直綫，取直綫上点的幂表現的幂指数，使之一个一个地移动。亦即令(0, 5, 10)为第一行，(1, 6, 11)为第二行，…。第二日，依上列置换有 $0\to1$，$5\to8$，$10\to14$，所以第一行是(1, 8, 14)。同样第二行是(2, 5, 6)，…。附表1中的記号 $K$ 表示作为 Kirkman 問題❶的推广而得到的 BIB。

## §11　差集合方法

对§10中 $d=1$ 的情形，当 $s$ 为偶数时，把 $\nu_1$ 条初始直綫上的点的幂指数排成

$$\begin{matrix} \alpha_{01} & \alpha_{11} & \alpha_{21} & \cdots\alpha_{t1} \\ \alpha_{02} & \alpha_{12} & \alpha_{22} & \cdots\alpha_{t2} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{0\nu_1} & \alpha_{1\nu_1} & \alpha_{2\nu_1} & \cdots\alpha_{t\nu_1} \end{matrix} \tag{11.1}$$

并以 $v$ 为模对每行作对称差如

$$\alpha_{01}-\alpha_{11},\ \alpha_{11}-\alpha_{01};\ \alpha_{01}-\alpha_{21},\ \alpha_{21}-\alpha_{01};\ \cdots, \tag{11.2}$$

❶ 德国人叫做 Steiner 系的問題。

則所有小于 $v$ 的差值只能出現一次。假如出現二次，那末 $0<c<v$，并且在同一直綫上有四点 $[x^\alpha]$，$[x^\beta]$，$[x^{\alpha+c}]$，$[x^{\beta+c}]$。例如設

$$\beta-\alpha \stackrel{\mathrm{d}}{=} d, \tag{11.3}$$

則 $[x^0]$，$[x^d]$，$[x^c]$，$[x^{c+d}]$ 在同一直綫上，而当以 $x^c$ 乘它們时，$[x^{2c}]$ 也在該直綫上，这意味着 $c$ 是循环数，因而与假定矛盾。又从其他行也不出現相同的差。因为，如果相同的差出現，那末这应是从相同的初始直綫生成的。因此，从

$$t(t+1)\nu_1=t(t^s-1)/(t-1)=v-1 \tag{11.4}$$

看出，1, 2, …, $v-1$ 至少必須出現一次。

一般，設有 $\rho$ 行 $\varkappa$ 列的整数，对各行作对称差，并以正整数 $v$ 为模来表示时，若除 0 以外小于 $v$ 的差值都出現 $\lambda$ 次，則这个整数矩陣叫做**差集合**。若存在一个差集合，則得到参数

$$v, \ k=\varkappa, \quad b=v\rho, \quad r=\varkappa\rho, \ \lambda \tag{11.5}$$

的 BIB。特别，对 $\rho=1$, $\lambda=1$ 的情形，設 $\varkappa=t+1$，則 $v=t^2+t+1$。对 $t\leqslant 1600$，人們已經驗証[1]，若 $t$ 不是素数或者素数冪，則差集合不存在；而对 $t>1600$，人們猜想，当 $t$ 不是素数或者素数冪时恐怕差集合也不存在。

現在問，由差集合方法可以得到而由上节的方法不能得到的 BIB 是否存在。試举这样一个例子：$v=9$, $k=4$, $\rho=2$, $\lambda=3$。把一行放入一个括弧，

$$(0, 1, 2, 4), \quad (0, 3, 4, 7).$$

这既不能从 $PG[s, t]$ 又不能从 $EG[s, t]$ 直接得到。本来，差集合只要求差的对称性，所以可用比域广义的代数系来考慮它。当然要求加法是封閉的。这样一个代数系对加法形成一个群，从而是满足减法唯一性的代数系，也就是一个模（加群）（参看附录）。关

[1] T. A. Evans and H. B. Mann: Sankhyā, 11 (1951), 356~364.

于模，我們有下列两个定理(R. C. Bose, 1939) [1]。

**定理 I** 把 $m$ 个品种 $x_1^{(u)}, x_2^{(u)}, \cdots, x_m^{(u)}$ 对应于阶 $n$ 的模 $\mathfrak{M}$ 中的每一元素 $x^{(u)}(u=0, 1, \cdots, n-1)$，称足碼相同的品种属于同一組 [2]。把这些品种放进 $t$ 个初始区組 $B_1, B_2, \cdots, B_t$，使同一区組只包含同一品种一次。假設

(i) 各个区組的大小都是 $k$，

(ii) 在 $t$ 个区組出現的全部 $kt$ 个品种中每有 $r$ 个品种属于 $m$ 組，从而有

$$kt=mr, \tag{11.6}$$

(iii) 若对各个区組作对称差，則差都对称地重复 $\lambda$ 次。

这里令 $\varphi$ 为 $\mathfrak{M}$ 的任意元素，从任意一个初始区組 $B_{l0} \stackrel{\mathrm{d}}{=} B_l$ 构造另一个区組 $B_{l\varphi}$，此处設 $B_{l\varphi}$ 中的品种 $x_i^{(v)}$ 由 $B_{l0}$ 中的品种 $x_i^{(u)}$ 定义为

$$x_i^{(v)}=x_i^{(u)}+\varphi. \tag{11.7}$$

于是 $B_{l\varphi}$ 全体形成一个 BIB，它的参数为

$$v=mn, \quad k, \ b=nt, \quad r=kt/m, \ \lambda. \tag{11.8}$$

这里，$x_i^{(u)}-x_i^{(v)}\ (u\neq v)$ 叫做 $[i, i]$ 型**純粹差**，$x_i^{(u)}-x_j^{(v)}\ (i\neq j)$ 叫做 $[i, j]$ 型**混合差**。設 $B_l$ 内有第 $i$ 組品种 $n_{il}$ 个。如果(1)由初始区組全体所产生的

$$n_{i1}(n_{i1}-1)+n_{i2}(n_{i2}-1)+\cdots+n_{it}(n_{it}-1) \tag{11.9}$$

个 $[i, i]$ 型純粹差中，$\mathfrak{M}$ 的每一非零元素不依賴于 $i$ 重复 $\lambda$ 次，以及(2)由初始区組全体所产生的

$$n_{i1}n_{j1}+n_{i2}n_{j2}+\cdots+n_{it}n_{jt} \tag{11.10}$$

[1] Bose [15]。——譯者注

[2] 这可能是解 Kirkman 問題时用到的 dicyclic 思想的推广。参看 Ball 的著书(§10 脚注)。附表 1 中的 $K$ 表示該书的解。

个 $[i, j]$ 型混合差中，$\mathfrak{M}$ 的每一元素不依赖于 $i, j$ 重复 $\lambda$ 次，那末称差**对称地重复**。

証明是簡单的。首先証明各品种的实施数为一定。由模的减法唯一性，当固定 $x_i^{(u)}$ 而使 $\varphi$ 变化 $n$ 次时，所有的 $x_i^{(v)}$ 都不相同。固定 $x_i^{(u)}$ 的 $u$，就有 $n$ 个第 $i$ 組的不同品种出現。若使 $u$ 变化 $r$ 次，則总共有 $rn$ 个第 $i$ 組的品种出現。故根据 (ii)，特定的 $x_i^{(v)}$ 恰好重复出現 $r$ 次。其次往証相遇数为一定。同一区組内的同一組的两品种 $x_i^{(v)}, x_i^{(v')}$ 形成**純粹对子**，属于同一区組内不同組的两品种 $x_i^{(u)}, x_j^{(u')} (i \neq j)$ 形成**混合对子**。形成純粹对子的必要与充分条件是，相应的 $x_i^{(u)}, x_i^{(u')}$ 相遇于任意一个初始区組 $B_l (l=1, \cdots, t)$ 中，并在 $\mathfrak{M}$ 中存在 $\varphi$，使得

$$x^{(v)}=x^{(u)}+\varphi, \quad x^{(v')}=x^{(u')}+\varphi. \tag{11.11}$$

取差便得 $\quad x^{(u)}-x^{(u')}=x^{(v)}-x^{(v')}=\mathfrak{M}$ 的特定元素。 (11.12)

根据(iii)，满足上列条件的 $x_i^{(u)}, x_i^{(u')}$ 必被包含于任意一个 $B_l$ $(l=1, \cdots, t)$ 共 $\lambda$ 次。$\varphi$ 由 $x^{(v)}-x^{(u)}$ 或者 $x^{(v')}-x^{(u')}$ 决定。对于混合对子也是如此。上面举的例子，是从以 9 为模的剩余类(参看附录)得到的模。

**例 1** 設

$$x_i-y_j \stackrel{\mathrm{d}}{=} (x-y)_{ij}. \tag{11.13}$$

从六个初始区組

$$(0_2, 1_2, 2_2), (1_1, 4_1, 0_2), (2_1, 3_1, 0_2),$$
$$(1_1, 4_1, 2_2), (2_1, 3_1, 2_2), (0_1, 0_2, 2_2)$$

得到的 [1, 1] 型和 [2, 2] 型純粹差对 $\mathfrak{M}$ 的元素 1, 2, 3, 4 都重复出現 $\lambda=2$ 次，而 [1, 2] 型和 [2, 1] 型混合差对 $\mathfrak{M}$ 的元素 0, 1, 2, 3, 4 也都重复出現 2 次。至于差的构造，例如以 $v=5$ 为模，从第一和第二区組得到

$$4_{22}, 3_{22}, 1_{22}, 4_{22}, 2_{22}, 1_{22};\ 2_{11}, 4_{12}, 3_{11}, 2_{12}, 1_{11}, 3_{12}.$$

由此得到具有下列参数的 BIB：

$$v=2\times5=10, \quad k=3, \quad b=5\times6=30, \quad r=9, \quad \lambda=2.$$

表

| 系統 | $v$ | $k$ | $b$ | $r$ | $\lambda$ |
|---|---|---|---|---|---|
| $A_1$ | $m(\lambda-1)+1=p^n$ | $\lambda$ | $mv$ | $mk$ | $\lambda$ |
| $B_1$ | $2am(2a\lambda+1)+1=p^n$ | $2a\lambda+1$ | $mv$ | $mk$ | $\lambda$ |
| $C_1$. | $2am(2a\lambda-1)+1=p^n$ | $2a\lambda$ | $mv$ | $mk$ | $\lambda$ |
| $D_2$ | $p^n+1=2k$ | $k$ | $2r=2(v-1)$ | $v-1$ | $k-1$ |
| $E_2'$ | $p^n+1=2k$ | $k$ | $2r=4(v-1)$ | $2(v-1)$ | $2(k-1)$ |
| $F_1$ | (在 $C_1$ 中令 $k=4$, $a=2$, $m=t$, $\lambda=1$ 得到的) | | | | |
| $F_2$ | $12t+4$ | 4 | $(4t+1)(3t+1)$ | $4t+1=p^n$ | 1 |
| $G_1$ | (在 $B_1$ 中令 $k=5$, $a=2$, $m=t$, $\lambda=1$ 得到的) | | | | |
| $G_2$ | $20t+5$ | 5 | $(5t+1)(4t+1)$ | $5t+1$ | 1 |
| $S_1$ | (在 $B_1$ 中令 $m=1$ 得到的。R. C. Bose 記为 $S_n$) | | | | |
| $T_2$ | (在 $B_1$ 中令 $k=3$, $a=1$, $m=t$, $\lambda=1$ 得到的) | | | | |
| $T_1$ | $6t+3$ | 3 | $(2t+1)(3t+1)$ | $3t+1$ | 1 |

❶ $q_s(s=1, 2, \cdots, a\lambda)$ 表示取模 $a$ 的剩余 $\lambda$ 次。

1)所有的 $x$ 都是 $GF[p^n]$ 的原始元素。2)若 $F_2$ 的解已知，則利用它很快得到 $G_2$。

3)对于 $k=3$, $v\leqslant100$ 的情形，参看 Ball 的著书 (§10 脚注)。

4)对于 $k=3$, $\lambda=2$ 的情形，$r=3u+2$ 或者 $3u$，若 $u$ 为偶数，則重迭 $T$ 系便得到。

## 11.1

| 附加条件 | 初始区組 |
|---|---|
| —— | $(0, x^i, x^{i+m}, x^{i+2m}, \cdots, x^{i+m(\lambda-2)})$, $i=0, 1, \cdots, m-1$ |
| $x^{2ams}-1 \stackrel{d}{=} x^{q_s}$❶ | $(x^{ai}, x^{ai+4am}, \cdots, x^{ai+4a^2m\lambda})$, $i=0, 1, \cdots, m-1$. 若 $m=1$, 則是 SBIB. |
| $x^{2ams}-1 \stackrel{d}{=} x^{q_s}$❷ | $(0, x^{ai}, x^{ai+2am}, \cdots, x^{ai+2am(2a\lambda-2)})$, $i=0, 1, \cdots, m-1$, 若 $m=1$, 則是 SBIB. |
| $k=2u$ | $(0, x^0, x^2, \cdots, x^{4(u-1)})$, $(\infty, x, x^3, \cdots, x^{4u-3})$, 全是 ARBIB. |
| —— | $(0, x^i, x^{i+2}, \cdots, x^{i+2k-4})$, $(\infty, x^{i+1}, x^{i+2}, \cdots, x^{i+2k-3})$, $i=0, 1$. 全是 RBIB. |
| $x^{4m}-1 \stackrel{d}{=} x^q$, $q=$奇数 | $(0, x^{2i}, x^{2i+4t}, x^{2i+8t})$, $i=0, 1, \cdots, m-1$. |
| $(x^a+1)/(x^a-1) \stackrel{d}{=} x^q$, $a, q$ 是奇数 | $(x_j^{2i}, x_j^{2i+2t}, x_{j+1}^{a+2i}, x_{j+1}^{a+2i+2t})$, $i=0, 1, \cdots, t-1$; $j=1, 2, 3$, $4\equiv1$. $(\infty, 0_1, 0_2, 0_3)$ |
| $q_2-q_1=$奇数 | $(x^{2i}, x^{2i+4t}, \cdots, x^{2i+16t})$, $i=0, 1, \cdots, t-1$. |
| $(x^a+1)/(x^a-1) \stackrel{d}{=} x^q$, $a, q$ 是奇数 | $(x_j^{2i}, x_j^{2i+2t}, x_{j+2}^{a+2i}, x_{j+2}^{a+2i+2t}, 0_j)$, $i=0, 1, \cdots, t-1$; $j=1, 2, \cdots, 5$, $6\equiv1$, $7\equiv2$. $(0_1, 0_2, 0_3, 0_4, 0_5)$. |
| $t \stackrel{d}{=} 2\tau+1$ | 在 $(i_1, (2\tau-i+1)_1, 0_2)$ 中使 $\tau$ 从 1 变到 $\tau$. 足碼变为 (1, 1, 2), (6, 6, 2), (6, 1, 5), (1, 6, 5), (2, 2, 3), (5, 5, 3), (5, 2, 4), (2, 5, 4), (3, 3, 1), (4, 4, 1), (4, 3, 6), (3, 4, 6). 又 $(0_1, 0_2, 0_3)$, $(0_1, 0_5, 0_4)$, $(0_6, 0_2, 0_4)$, $(0_3, 0_6, 0_5)$, $(\infty, 0_1, 0_6)$, $(\infty, 0_2, 0_5)$, $(\infty, 0_3, 0_4)$. |
| —— | $(i_j, (2t-i+1)_j, 0_{j+1})$, $(0_1, 0_2, 0_3)$, $i=1, 2, \cdots, t$; $j=1, 2, 3$, $4\equiv1$. |

● $q_s$ $(s=1, 2, \cdots, a\lambda-1)$ 表示取模 $a$ 的剩余为 0 的 $(\lambda-1)$ 次,其余 $\lambda$ 次。

当 $u=2t+1$ 时, $r=6t+5$ ($E_1$ 系) 或者 $6t+3$ ($E_2$ 系),对这种情形, R. C. Bose (1939) 有所研究。对这些情形,所有解都导致 $b>100$, 所以这里从略。

5) 从参数看来,迭合 $D_2$ 系可得到 $E_2'$ 系。

**定理 II** 給阶 $n$ 的模 $\mathfrak{M}$ 中的元素 $x^{(u)}(u=0, 1, 2, \cdots, n-1)$ 添上一个新元素 $\infty$，并定义[1]

$$\infty+x^{(u)}=\infty, \tag{11.14}$$

此处 $u$ 是任意的。設有 $t+s$ 个初始区組 $B_1, B_2, \cdots, B_t$; $B'_1, B'_2, \cdots, B'_s$ 并且

(i) 每一 $B_l$ 包含 $x_i^{(u)}$ 中不同 $k$ 个，$B'_h$ 包含 $x_i^{(u)}$ 中不同 $k-1$ 个和 $\infty$。

(ii) 在 $B_1, B_2, \cdots, B_t$ 中出現的 $kt$ 个品种中，每有 $ns-\lambda$ 个分属于依定理 I 意义的 $m$ 組，而在 $B'_1, B'_2, \cdots, B'_s$ 中出現的 $s(k-1)$ 个品种中，每有 $\lambda$ 个分属于上述意义的 $m$ 組。从而

$$kt=m(ns-\lambda), \quad s(k-1)=m\lambda. \tag{11.15}$$

(iii) 令 $B''_h$ 表示从 $B'_h$ 除去 $\infty$ 后的区組，則从 $B_l$, $B''_h$ 等 $t+s$ 个区組得到的差都对称地重复着 $\lambda$ 次。

这里利用 $\mathfrak{M}$ 中的任意元素 $\varphi$，設 $B_{l0}\stackrel{d}{=}B_l$, $B'_{h0}\stackrel{d}{=}B'_h$ 为初始区組，如定理 I 那样，由

$$x^{(v)}=x^{(u)}+\varphi, \quad \infty=\infty+\varphi \tag{11.16}$$

来构造 $B_{l\varphi}$, $B'_{h\varphi}$. 所有这些区組全体給出一个 BIB，它的參数如下：

$$v=mn+1, \quad k, \quad b=n(s+t), \quad r=ns, \lambda. \tag{11.17}$$

証明也是简单的。$x_i^{(u)}$ 在 $B_{l\varphi}$ 系統中实施 $ns-\lambda$ 次，在 $B'_{h\varphi}$ 系統中实施 $\lambda$ 次，于是合計起来的实施数为 $ns$. $\infty$ 只在 $B'_{h\varphi}$ 系統中实施 $ns$ 次。欲考虑相遇数，除定理 I 中的純粹对子和混合对子以外，还要定义以 $\infty$ 为对象的**附加对子**。附加对子只出現于 $B'_{h\varphi}$ 系統，它的次数是 $\lambda$. 至于純粹对子及混合对子也都出現 $\lambda$ 次，只須留

[1] 这个 $\infty$ 可能相当于 Kirkman 問题的循环解的圆中心，亦即不动点。參看 Ball 的著书(§10 脚注)。

意下述这样一个事实就明显:在定理I的証明中,証明相遇数λ和实施数$r$的解的存在性时并不要求区組大小为一定。

利用定理I和II得到的BIB,在附表1中用記号$D$表示之。

在表11.1的系統中,足碼1和2分別表示由定理I和II得到的BIB. 从$A_1$到$E'_2$应归功于D. A. Sprott (1956)❶,其余应归功于R. C. Bose (1939)❷。

## §12 BIB的变形法

从一个BIB导出另一个非同构的BIB,这叫做BIB的变形法。現在人們知道三种方法。

(i) **切除法** 也称剩余法。这是从$PG[s, t]$构造$EG[s, t]$时已經用到的方法。一般,从一个SBIB中除掉一个区組,同时从其余区組中除去这个区組所包含的品种。

(ii) **誘导法** 若原来的設計是一个SBIB,并且$\lambda>1$,则只留下特定一个区組中的品种,而从各个区組除去其余品种,同时除去那个特定区組。

(iii) **相补法** 若原来的設計是一个BIB,则把不包含于第$i$个区組$B_i$内的那些品种来构造新区組$B'_i$,此处$i=1, 2, \cdots, b$. 这些新区組全体形成一个BIB.

用原設計的参数来表示上列方法得到的新参数,我們有表12.1❸。

考虑切除法的逆。当BIB的参数满足

$$r=k+\lambda,\quad v\lambda=k(k+\lambda-1),\quad b\lambda=(k+\lambda)(k+\lambda-1) \quad (12.1)$$

---

❶ Sprott[57].——譯者注

❷ Bose[15].——譯者注

❸ 欲說明由切除法和誘导法得到的設計实在是一个BIB,必須指出这样一个性质:在SBIB中任意两个区組恰好公有λ个品种。証明見例如Mann[6],124,或者本书第4章等价性問題的証明(15.33)。——譯者注

表 12.1

| 系統 | $v$ | $k$ | $b$ | $r$ | $\lambda$ | 附表1中的記号 |
|---|---|---|---|---|---|---|
| 切除法 | $v-k$ | $k-\lambda$ | $v-1$ | $k$ | $\lambda$ | $B$ |
| 誘导法 | $k$ | $\lambda$ | $v-1$ | $k-1$ | $\lambda-1$ | $d$ |
| 相补法 | $v$ | $v-k$ | $b$ | $b-r$ | $b-2r+\lambda$ | $C$ |

时，这个設計 $D$ 嵌入 SBIB 的必要与充分条件是，存在一組区組 $S_1, S_2, \cdots, S_{k+\lambda}$，使得(i)每个 $S_j$ 包含 $D$ 中的 $k+\lambda-1$ 个区組，(ii)一个 $S_j$ 总共包含 $D$ 中的各个品种 $\lambda$ 次，(iii) $S_i$, $S_j$ $(i\neq j)$ 公有 $D$ 中的 $\lambda-1$ 个区組，以及 (iv) $D$ 中的任意一个区組包含于 $\lambda$ 个 $S_j$ 中 (M. Hall, Jr., W. S. Connor, 1954)❶。

❶ Hall-Connor[82]。最近 Shrikhande[54]对 $\lambda=2$ 的情形給了一个构造性的証明。——譯者注

# 第3章 多因子試驗

## §13 多因子試驗[1]

在§2的BIB的构造模型中，我們同时考慮了品种和区組这两个**因子**[2]，其中品种有 $v$ 种变化，区組有 $b$ 种变化。这些变化分别叫做 $v$ 个**水平**和 $b$ 个**水平**。对完全区組設計，試驗本身則叫做 $v\times b$ 型試驗。水平对应于质的或者量的差异。一般地，例如同时考慮氮肥处理 $A_1$，磷肥处理 $A_2$，鉀肥处理 $A_3$，…，$A_n$ 等多个因子，它們每亩使用量分别为 $p_1, p_2, \cdots, p_n$ 个水平，而当以每亩收成为目标来比较肥料效应时，則称为

$$p_1\times p_2\times\cdots\times p_n(=N) \tag{13.1}$$

**型多因子試驗**。在工厂中通常被利用的是 $N=2^n$ 或 $3^n$ 的情形，而 $N=p^{n'}\times q^{n''}\times r^{n'''}\times\cdots$的情形也被利用。令 $T(y_1, y_2, \cdots, y_n)$ 表示对应于第 $i$ 个因子 $A_i$ 取水平 $y_i$ 时的**处理組合** $(y_1, y_2, \cdots, y_n)$ 的观察值的隨机变数，$C(y_1, y_2, \cdots, y_n)$ 表示仅由这些水平而定的常数。考慮綫性組合

$$L_C\stackrel{\text{d}}{=}\sum C(y_1, y_2, \cdots, y_n)T(y_1, y_2, \cdots, y_n), \tag{13.2}$$

此处 $\sum$ 是对所有可能組合 $(y_1, y_2, \cdots, y_n)$ 的求和，而 $y_i$ 的变域为 $1, 2, \cdots, p_i$。若上式系数 $C$ 的和为 0，則称 $L_C$ 为**样本对比**。若不致同参数对比混淆，則簡称为对比。考慮另一对比

$$L_D\stackrel{\text{d}}{=}\sum D(y_1, y_2, \cdots, y_n)T(y_1, y_2, \cdots, y_n). \tag{13.3}$$

若(13.2)和(13.3)对应系数的乘积和

---

[1] 也称多种方式設計(higher way layout)。——譯者注

[2] 增山[7]，計画篇有詳細的解說。

$$\sum C(y_1, y_2, \cdots, y_n) D(y_1, y_2, \cdots, y_n) = 0, \qquad (13.4)$$

則称对比 $L_C$ 和 $L_D$ 互为**正交**。适当地給組合 $(y_1, y_2, \cdots, y_n)$ 記上 1 到 $N$ 的号碼，按这个号碼的顺序，把 $C$, $T$, $D$ 排列起来看做 $N$ 維 Euclid 空間中的矢量的正交分量，这样就容易理解正交的意义。因此，只要是綫性組合，即使不是对比，也可以定义正交性。在这个意义上，由于任意对比的系数和都为 0，所以它正交于观察値的总和

$$G \stackrel{\mathrm{d}}{=} \sum T(y_1, y_2, \cdots, y_n). \qquad (13.5)$$

也可以說，它与总平均 $M \stackrel{\mathrm{d}}{=} \frac{G}{N}$ 正交。

一般，設有 $N$ 个随机变数 $X_1, X_2, \cdots, X_N$，又令 $M$ 为总平均，則

$$\begin{aligned} S_X &\stackrel{\mathrm{d}}{=} (X_1 - M)^2 + (X_2 - M)^2 + \cdots + (X_N - M)^2 \\ &= X_1^2 + X_2^2 + \cdots + X_N^2 - NM^2 = \boldsymbol{X}^2 - (\boldsymbol{X} \cdot \boldsymbol{e}_0)^2 \end{aligned} \qquad (13.6)$$

叫做**变差**或者**变差平方和**，此处 $\boldsymbol{X}$ 是以 $X_1, X_2, \cdots, X_N$ 为正交分量的 $N$ 維 Euclid 空間內的矢量，$\boldsymbol{e}_0$ 是分量都为 $\frac{1}{\sqrt{N}}$ 的同一空間內的单位矢量。在这个空間中，包含 $\boldsymbol{e}_0$ 在內，形成一完备正交单位矢量系 $\boldsymbol{e}_0, \boldsymbol{e}_1, \cdots, \boldsymbol{e}_{N-1}$，此处

$$\boldsymbol{e}_i \cdot \boldsymbol{e}_j = \delta_{ij}, \quad i, j = 0, 1, 2, \cdots, N-1. \qquad (13.7)$$

利用上列諸式，便得到

$$S_X = \boldsymbol{X}^2 - (\boldsymbol{X} \cdot \boldsymbol{e}_0)^2 = (\boldsymbol{X} \cdot \boldsymbol{e}_1)^2 + (\boldsymbol{X} \cdot \boldsymbol{e}_2)^2 + \cdots + (\boldsymbol{X} \cdot \boldsymbol{e}_{N-1})^2. \qquad (13.8)$$

由于 $\boldsymbol{e}_i$ $(i>0)$ 与 $\boldsymbol{e}_0$ 正交，所以

$$L_i \stackrel{\mathrm{d}}{=} \boldsymbol{X} \cdot \boldsymbol{e}_i \qquad (13.9)$$

是对比。由此可知，$S_X$ 可以分解为相互正交的对比 $L_1, L_2, \cdots,$

$L_{N-1}$ 的平方和。若每一 $X_1, X_2, \cdots, X_N$ 对应于 $k$ 个相互独立观察值的和，則定义 $\frac{S_X}{k}$ 为变差。在(13.6)中，

$$\boldsymbol{X}\cdot\boldsymbol{e}_0=\sqrt{N}M \tag{13.10}$$

是对 $\boldsymbol{X}$ 的一个綫性約束条件，而一般有綫性約束条件

$$\boldsymbol{X}\cdot\boldsymbol{q}_\alpha=\xi_\alpha, \quad \alpha=1, 2, \cdots, p(<N), \tag{13.11}$$

此处令 $\boldsymbol{q}_1, \boldsymbol{q}_2, \cdots, \boldsymbol{q}_p$ 为綫性独立。設

$$a_{\alpha\beta}\overset{\mathrm{d}}{=}\boldsymbol{q}_\alpha\cdot\boldsymbol{q}_\beta, \tag{13.12}$$

則因 $(a_{\alpha\beta})$ 的逆矩陣 $(A_{\alpha\beta})$ 存在，所以設

$$\boldsymbol{Q}_\alpha\overset{\mathrm{d}}{=}A_{\alpha1}\boldsymbol{q}_1+A_{\alpha2}\boldsymbol{q}_2+\cdots+A_{\alpha p}\boldsymbol{q}_p, \tag{13.13}$$

則

$$\boldsymbol{Q}_\alpha\cdot\boldsymbol{q}_\beta=\delta_{\alpha\beta}. \tag{13.14}$$

設

$$S_{X_p}\overset{\mathrm{d}}{=}\left(\boldsymbol{X}-\sum_{\alpha=1}^{p}\xi_\alpha\boldsymbol{Q}_\alpha\right)^2. \tag{13.15}$$

若 $X_1, X_2, \cdots, X_N$ 为相互独立，并都具有方差 $\sigma^2$，則

$$E\{S_{X_p}\}=(N-p)\sigma^2. \tag{13.16}$$

$f\overset{\mathrm{d}}{=}N-p$ 叫做变差 $S_{X_p}$ 的**自由度**，或者**无偏方差**

$$s^2\overset{\mathrm{d}}{=}\frac{S_{X_p}}{N-p}$$

的自由度❶。自由度这个名称，其意义与 W. Gibbs(1874～1878)的相律的情形相同。$S_{X_p}$ 可以分解为相互正交的 $f$ 个对比的平方和。

設有两个变差 $S_1$ 和 $S_2$，适当地分别把它們分解为对比的平方和，若一个变差的任意对比与另一个变差的任意对比正交，則称变差 $S_1$ 和 $S_2$ 互为**正交**。若 $S_1$ 和 $S_2$ 不包含公共随机变数，則从

❶ 这个不依賴于分布型的定义是由笔者 (1944) 給出的，但是自由度的概念应归功于 Fisher (1925).

随机变数的乘积空間显然看出，$S_1$ 和 $S_2$ 互为正交。

現在，設有 $N=p_1p_2r$ 个相互独立的对应于观察值的随机变数，并无重复地把它們分为 $p_1$ 行 $p_2$ 列的 $p_1p_2$ 个組，使每組都包含 $r$ 个随机变数。这时，取任意两行，求其中一行所包含的 $p_2r$ 个变数之和与另一行所包含的 $p_2r$ 个变数之和的差，則这是一个对比。这叫做这两行之間的**行間对比**。同样，取任意两列，求其中一列所包含的 $p_1r$ 个变数之和与另一列所包含的 $p_1r$ 个变数之和的差。这叫做这两列之間的**列間对比**。任意的行間对比与任意的列間对比互为正交。因此，对 $p_1$ 行分别求得的和之間的变差即自由度 $p_1-1$ 的**行間变差**与对 $p_2$ 列分别求得的和之間的变差即自由度 $p_2-1$ 的**列間变差**互为正交。这叫做**正交修正原理**(R. C. Bose, 1947) ❶。根据这个原理，若在多因子設計中着眼于 $n$ 个因子中的任意两个因子 $A_i$ 和 $A_j$，把 $y_i$, $y_j$ 相等的观察值放进同一組，并分为 $p_i$ 行 $p_j$ 列，則其中一个因子 $A_i$ 的 $p_i$ 个水平間的变差与另外一个因子 $A_j$ 的 $p_j$ 水平間的变差互为正交，此处 $r=\dfrac{N}{p_ip_j}$.

关于某个对比式子，所謂它的系数不依賴于因于 $A_i$ 以外的因子水平，乃是指对 $A_i$ 的水平 $y_i$ 为一定的所有处理，系数均相等。这时，称这个对比属于**主要效应** $A_i$. 所謂对比属于**二因子交互作用** $A_i\times A_j$ $(i\neq j)$，乃是指：(i) 这个对比的系数不依賴于二因子 $A_i$ 和 $A_j$ 以外的因子水平，以及 (ii) 这个对比与属于主要效应 $A_i$ 的任意对比和属于主要效应 $A_j$ 的任意对比都为正交。同样可以定义属于**三因子交互作用** $A_i\times A_j\times A_k$ $(i\neq j\neq k\neq i)$ 的对比以及属于更**高阶交互作用**的对比。条件是下列两个：(i) 問題的交互作用的对比的系数不依賴于其他因子水平，(ii) 問題的交互作用的对比正交于每一属于只含有与該交互作用相同的字母 $A$ 的低阶交

❶ Bose [17]. ——譯者注

互作用，此处把主要效应看做一因子交互作用。下面我們只考虑

$$p_1=p_2=\cdots=p_n=t\ (=\text{素数或者素数幂}) \qquad (13.17)$$

的情形❶。

首先考虑 $t$ 为素数 $p$ 的情形。令 $y_1, y_2, \cdots, y_n$; $g_1, g_2, \cdots, g_n$; $m$ 为 $GF[p]$ 的元素，考虑 $EG[n, p]$ 中的点 $(y_1, y_2, \cdots, y_n)$ 满足

$$g_1y_1+g_2y_2+\cdots+g_ny_n\equiv m \pmod p, \qquad (13.18)$$

此处設系数 $g$ 不全为 0. 当固定 $[g_1, g_2, \cdots, g_n]$ 和 $m$ 时，共有 $p^{n-1}$ 个点。若只使 $m$ 取 $p$ 个值，則 $EG[n, p]$ 中所有的点都出現一次。考虑固定 $[g_1, g_2, \cdots, g_n]$ 和 $m$ 时由各点作的試驗得到的观察值，求这些 $p^{n-1}$ 个观察值的和，并把它看做随机变数 $T_m$ 的实現值。**对比集合** $T_0, T_1, \cdots, T_{p-1}$ 之間的变差

$$S=(T_0^2+T_1^2+\cdots+T_{p-1}^2)/p^{n-1}-G^2/N \qquad (13.19)$$

叫做属于处理效应 $[g_1, g_2, \cdots, g_n]$ 的变差。令 $\rho$ 为 $GF[p]$ 中的非零元素，則当使 $m$ 从 0 变到 $p-1$ 时 $\rho m$ 与适当地以 0 到 $p-1$ 代入的点一致，所以属于 $[\rho g_1, \rho g_2, \cdots, \rho g_n]$ 的变差与 $\rho=1$ 时的变差一致。这就是說，效应記号 $[g_1, g_2, \cdots, g_n]$ 具有射影坐标的性质，所以可由 $PG[n-1, p]$ 中的一点来表达。

**例 1** 对于 $3^2$ 型，例如有表 13.1。

表 13.1

| 效应 | 点 | | 对比集合 |
|---|---|---|---|
| [1 0] | $y_1=$ | 0　(0 0), (0 1), (0 2) | $T(0\ 0)+T(0\ 1)+T(0\ 2)$ |
| | | 1　(1 0), (1 1), (1 2) | $T(1\ 0)+T(1\ 1)+T(1\ 2)$ |
| | | 2　(2 0), (2 1), (2 2) | $T(2\ 0)+T(2\ 1)+T(2\ 2)$ |
| [1 2] | $y_1+2y_2=$ | 0　(0 0), (1 1), (2 2) | $T(0\ 0)+T(1\ 1)+T(2\ 2)$ |
| | | 1　(1 0), (2 1), (0 2) | $T(1\ 0)+T(2\ 1)+T(0\ 2)$ |
| | | 2　(2 0), (0 1), (1 2) | $T(2\ 0)+T(0\ 1)+T(1\ 2)$ |

❶ 关于一般非对称多因子試驗，參看 Wald [10]，K. R. Nair and C. R. Rao: J. R. S. S., ser. B, **10** (1948), 109～131.

在射影坐标中，不失普遍性地可以用 1 来代替从左算起第一个坐标不为 0 的数。

所謂属于 $[g_1, g_2, \cdots, g_n]$ 的变差，乃是指当只有 $g_i$ 不为 0 时属于主要效应 $A_i$ 的对比間的变差。这叫做**主要效应 $A_i$ 的变差**。自由度是 $p-1$ 个。若只有 $g_i$ 和 $g_j$ $(i\neq j)$ 不为 0，則記属于它們的变差为 $S(i, j; g_i, g_j)$。固定坐标号碼 $i, j$，使 $g_i, g_j$ 不为 0 地变化，作可能組合 $[g_i, g_j]$，并对其中作为射影空間的所有不同的 $p-1$ 个点求和，便得到**二因子交互作用 $A_i\times A_j$ 的变差**

$$S_{A_i\times A_j}=\sum S(i, j; g_i, g_j)\quad (i\neq j). \tag{13.20}$$

自由度是 $p-1$ 的 $(p-1)$ 倍。同样，三因子交互作用 $A_i\times A_j\times A_k$ $(i\neq j\neq k\neq i)$ 的变差是

$$S_{A_i\times A_j\times A_k}=\sum S(i, j, k; g_i, g_j, g_k). \tag{13.21}$$

这在射影坐标 $[g_i, g_j, g_k]$ 中令任意坐标都不为 0，并对其中所有可能不同的 $(p-1)^2$ 个点求和便得到。自由度是 $(p-1)^3$ 个。从几何学来看，主要效应相当于 $PG[n-1, p]$ 中一点的对比集合的变差之和；二因子交互作用相当于 $(p-1)$ 个点的对比集合的变差之和，这 $(p-1)$ 个点是在結合着表示主要效应的两点的直綫上的、但除这两点以外的点；三因子交互作用相当于 $(p-1)^2$ 个点的对比集合的变差之和，这 $(p-1)^2$ 个点是在結合着表示主要效应的三点的平面上的、但除去在結合着这三点的直綫上的点以外的点。每一点的自由度总是 $p-1$ 个。

对于一般情形，把 $EG[n, t]$ 中的点 $(y_1, y_2, \cdots, y_n)$ 对应于处理組合，并把除原点

$$e_0=(0, 0, \cdots, 0) \tag{13.22}$$

以外的 $t^n-1$ 个点分为每有 $\theta$ 个点的 $t-1$ 組，此处

$$\theta\overset{\text{d}}{=}\frac{t^n-1}{t-1}. \tag{13.23}$$

若第 $i$ 个坐标为 1 其余坐标为 0 的点表为

$$e_i \stackrel{\Delta}{=} (0,\ 0,\ \cdots,\ 1,\ \cdots,\ 0) \quad (i=1,\ 2,\ \cdots,\ n), \tag{13.24}$$

則第1組的点可由

$$e_i + a_{i,\,i+1}e_{i+1} + a_{i,\,i+2}e_{i+2} + \cdots + a_{in}e_n \tag{13.25}$$

所表达的点組成。上式总共有 $t^{n-i}$ 个,对 $i$ 求和恰好得 $\theta$ 个点,此处設系数为 $GF[t]$ 中的元素。令 $\rho$ 为 $GF[t]$ 中的非零元素,并使第 $\rho$ 組的点为第1組各点的 $\rho$ 倍。在第1組中按 $e_1, e_2, \cdots, e_n$ 的順序排列,其余当把坐标看做处理效应記号时,按二因子交互作用,三因子交互作用,……的順序排列,而在同是二因子交互作用中,則按辞典式的順序排列。

表13.2 $t=3,\ n=2$ 的例子

| | 卡片号碼 | [1 0] | [0 1] | [1 1] | [1 2] |
|---|---|---|---|---|---|
| | 0 | 0 | 0 | 0 | 0 |
| 第1組 | 1 | 1 | 0 | 1 | 1 |
| | 2 | 0 | 1 | 1 | 2 |
| | 3 | 1 | 1 | 2 | 0 |
| | 4 | 1 | 2 | 0 | 2 |
| 第2組 | 5 | 2 | 0 | 2 | 2 |
| | 6 | 0 | 2 | 2 | 1 |
| | 7 | 2 | 2 | 1 | 0 |
| | 8 | 2 | 1 | 0 | 1 |

把这些分量排列起来,便得到 $N$ 行 $n$ 列的矩陣。这还可以往右側扩大到第 $\theta$ 列。例如欲求第 $i$ 列第 $l$ 行的元素,先看第 $i$ 行左端的 $n$ 列 $(i \leqslant \theta)$。若那是

$$g_1e_1 + g_2e_2 + \cdots + g_ne_n, \tag{13.26}$$

則令 $(y_1,\ y_2,\ \cdots,\ y_n)$ 为第 $l$ 行左端的元素,并求

$$g_1y_1 + g_2y_2 + \cdots + g_ny_n, \tag{13.27}$$

然后令它为第 $i$ 列第 $l$ 行的元素。用 $[g_1,\ g_2,\ \cdots,\ g_n]$ 作为这一列的标号。这样便得到 $N=t^n$ 行 $k=\theta$ 列的矩陣。第0行用相同方

法扩大$e_0$得到。第1組是$[\theta, \theta]$型对称矩陣,第$\rho$組是它的$\rho$倍。适当地給$GF[t]$的元素記上号碼使之暗号化,可把一行写成一張穿孔卡片。各卡片头$n$列的暗号規定处理組合。在試驗前要先使試驗順序或者位置随机化。把处理組合的試驗結果記入該張卡片,对具有标号$[g_1, g_2, \cdots, g_n]$的列把$N$張卡片全体分为$t$組,則各組的观察值的和給出属于这个記号的对比集合。求这个对比集合的変差,則得到属于这个記号的変差❶。根据正交修正原理,不同两列的変差互为正交。依这个意义把这个$N$行$\theta$列的矩陣叫做**正交陣列表**。从几何学来看,一列对应于$PG[n-1, t]$中的一点。

这里考虑$v=t^n$个品种,把品种号碼对应于上述卡片号碼。对各列把品种分为$t$組,并把一組放进一个区組,則得到参数

$$v=t^n,\ k=t^{n-1},\ b=t\theta,\ r=\theta,\ \lambda=(t^{n-1}-1)/(t-1) \quad (13.28)$$

的ARBIB. 取任意两列,把同行的两个值看做矢量的两个分量,并取对应于同一矢量的$t^{n-2}$个品种为一組,則得

$$v=t^n,\quad k=t^{n-2},\quad b=t^2\theta,\quad r=\theta,\quad \lambda=(t^{n-2}-1)/(t-1). \quad (13.29)$$

同样取任意三列或者四列,……,都可得到BIB. 最后得到的是

$$v=t^n,\quad k=t,\quad b=t^{n-1}\theta,\quad r=\theta,\quad \lambda=1. \quad (13.30)$$

这些都是RBIB. 称它們为**序貫混杂系統的**BIB❷.

## §14 正交陣列表❸

一般,当从$N$行$k$列矩陣取任意$d$列$(2\leqslant d<k)$,并把同行上的$d$个元素按其順序看做$t$进法$d$位数时❶,若所有$t^d$个可能的

❶ 参看增山[7],計画篇和增山[8]。
❷ 增山[7]計画篇附录有詳細的解說。
❸ 关于正交陣列表的历史,可参看增山[39]。——譯者注
❶ 在上节看做矢量,但沒有本质上的差异。

数都分别出現 λ 次，則称这个矩陣为**大小** $N$，**約束数** $k$，**水平数** $t$，**强度** $d$ 和**指数** λ 的**正交陣列表**(略称 OA)，記作$(\boldsymbol{N}, \boldsymbol{k}, \boldsymbol{t}, \boldsymbol{d})$。从定义有

$$N=\lambda t^d. \tag{14.1}$$

当給定 $N$, $t$ 和 $d$ 时，对 $k$ 有上限。上节的正交陣列表是

$$N=t^n,\quad k=(t^n-1)/(t-1),\quad t,d=2,\quad \lambda=t^{n-2}. \tag{14.2}$$

特别，

$$N=t^2,\quad k=3,\quad d=2 \tag{14.3}$$

的正交陣列叫做**边长** $t$ **的拉丁方**，

$$N=t^3,\quad k=4,\quad d=2 \tag{14.4}$$

的叫做边长 $t$ 的**立方**，

$$N=t^2,\quad k=4,\quad d=2 \tag{14.5}$$

的叫做**希腊·拉丁方**或者 **Euler 方**[1][2]。从此令第一列为行号碼，第二列为列号碼，第三列为拉丁字母(連队)号碼，第四列为希腊字母(軍衔)号碼，則得如表 14.1 那种排列(参看 §3)。

表 14.1

| | | |
|---|---|---|
| $A\alpha$ | $B\gamma$ | $C\beta$ |
| $B\beta$ | $C\alpha$ | $A\gamma$ |
| $C\gamma$ | $A\beta$ | $B\alpha$ |

从 $PG[n-1, t]$ 中选取 $k$ 个点，使任意 $d$ 个点为綫性独立，則得到下述强度 $d$ 的 OA。記

$$[g_{1i}, g_{2i}, \cdots, g_{ni}]\quad i=1, 2, \cdots, k \tag{14.6}$$

为 $GF[t]$ 的元素排成的 $k$ 个点，又設

$$(y_1, y_2, \cdots, y_n)\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1k} \\ g_{21} & g_{22} & \cdots & g_{2k} \\ \vdots & \vdots & & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nk} \end{pmatrix}=(m_1, m_2, \cdots, m_k). \tag{14.7}$$

使 $y$ 变化便得到右边的 $N=t^n$ 个矢量的分量，把这些分量依序排起来而得的 $N$ 行 $k$ 列就是欲求的 OA。

---

[1] 参看 M. P. A. MacMahon: Combinatory Analysis, **1** (1915), **2** (1916), Cambridge Univ., Ball 的著书(§10 脚注)；Mann [6]；増山 [7] 推定篇。

[2] 还可参看刘璋温 [35]。——譯者注

Euler 方可以看做是把拉丁字母所成的拉丁方和希腊字母所成的拉丁方迭合起来的方陣。上下的差异对应于所排字母的右左的差异。如表 14.1 那样,把两个拉丁方迭合起来成一 Euler 方的,叫做互为**正交**的拉丁方。正交拉丁方的存在不一定要求边长 $t$ 为素数。設 $t$ 的素因数分解为

$$t \overset{d}{=} p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}. \tag{14.8}$$

令 $y^{(j)}$ 为 $GF[p_j^{e_j}]$ 的任意元素,并設

$$Y \overset{d}{=} [y^{(1)}, y^{(2)}, \cdots, y^{(m)}]. \tag{14.9}$$

設点 $Y$ 的結合律为

$$Y_1 \circ Y_2 \overset{d}{=} [y_1^{(1)} \circ y_2^{(1)}, y_1^{(2)} \circ y_2^{(2)}, \cdots, y_1^{(m)} \circ y_2^{(m)}], \tag{14.10}$$

此处 $\circ$ 表加法 $+$ 或乘法 $\times$. 若坐标中有一为 0,把它除掉后,則存在着逆元素。存在逆元素的元素称为**正則**。单位元素也存在。这点集滿足从域公理系中去掉除法唯一性的环的公理系(参看附录)。

以后記 $GF[p_j^{e_j}]$ 的元素为

$$y_0^{(j)} \overset{d}{=} 0,\ \ y_1^{(j)} \overset{d}{=} 1,\ \ y_2^{(j)}, \cdots, y_{p_j^{e_j}-1}^{(j)}. \tag{14.11}$$

設 $0<j\leqslant k=\min\limits_j (p_j^{e_j}-1)$,又設

$$Y_j \overset{d}{=} [y_j^{(1)}, y_j^{(2)}, \cdots, y_j^{(m)}], \tag{14.12}$$

則 $Y_j$ 为正則,若 $j \neq l$, 則 $(Y_j - Y_l)$ 也为正則。定义

$$Y_0 \overset{d}{=} [0, 0, \cdots, 0], \tag{14.13}$$

并对其他的 $Y$ 适当地記上号碼 $j+1, j+2, \cdots, t-1$. 不同的点 $Y_i$ 共有 $t$ 个。現在,当固定 $Y_j (0<j\leqslant k)$ 时,

$$(L_j)\quad \begin{matrix} Y_0Y_j+Y_0 & Y_0Y_j+Y_1 & \cdots & Y_0Y_j+Y_{t-1} \\ Y_1Y_j+Y_0 & Y_1Y_j+Y_1 & \cdots & Y_1Y_j+Y_{t-1} \\ \vdots & \vdots & & \vdots \\ Y_{t-1}Y_j+Y_0 & Y_{t-1}Y_j+Y_1 & \cdots & Y_{t-1}Y_j+Y_{t-1} \end{matrix} \tag{14.14}$$

給出一个拉丁方。并且若 $j \neq l$, 則 $(L_j)$ 与 $(L_l)$ 为正交。首先上列

矩陣的元素为形状

$$y=xm+b, \tag{14.15}$$

当固定 $m=Y_j$ 时，在行上不同的是 $b$，在列上不同的是 $x$。因此在同一行上显然不存在同一元素。假設在同一列上有两个元素相同，例如

$$Y_a Y_j + Y_i = Y_c Y_j + Y_l. \tag{14.16}$$

由于 $Y_j$ 为正則，存在着逆元素，所以从上式减去 $Y_l$，再从右边乘上 $Y_j^{-1}$，便可推出 $Y_a=Y_c$。其次假設 $j\neq l$ 及

$$Y_\alpha Y_j + Y_\beta = Y_\sigma Y_j + Y_\tau, \quad Y_\alpha Y_l + Y_\beta = Y_\sigma Y_l + Y_\tau, \tag{14.17}$$

則有

$$Y_\alpha (Y_j - Y_l) = Y_\sigma (Y_j - Y_l). \tag{14.18}$$

由于 $(Y_j-Y_l)$ 为正則，存在着逆元素。因此得到 $Y_\alpha=Y_\sigma$。以此代入(14.17)，便可推出 $Y_\beta=Y_\tau$。故当 $j\neq l$ 时 $(L_j)$ 与 $(L_l)$ 为正交。因此，令 $p^e$ 为 $t$ 的素因数中最小的一个，則至少存在 $k=p^e-1$ 个互为正交的拉丁方❶。从这个証明不难看出，作为出发点的代数系不必要是 Galois 域，又不用到乘法的可換律和左側分配律，所以从 V-W 平面的对偶平面可以构造正交拉丁方。

正交拉丁方至多只有 $t-1$ 个。令 $L_1$ 和 $L_2$ 为任意两个正交拉丁方，分别把它們的第一行改排为 0, 1, …, $t-1$ 的順序。这种改排总是可能的，因为只要交换各个拉丁方中的字母卽可。設 $L_1'$ 和 $L_2'$ 为改排后的正交拉丁方。把它們迭起来，則 0 0, 1 1, 2 2。…, $(t-1)$ $(t-1)$ 排在第一行，所以在第二行第一列不可能包含 0，而且也不可能排两个相同的数。故至多只存在 $(t-1)$ 个互为正交的拉丁方。当 $t$ 为素数或者素数冪时，依上述方法可以构造到这个上限。这 $(t-1)$ 个拉丁方全体叫做**完备正交拉丁方系**❷。剩下的

---

❶ 这个結果应归功于 Mann [38]。——譯者注

❷ 最近 Shrikhande[55] 証明了：对 $t\neq 4$，$(t-3)$ 个正交拉丁方的存在蘊涵完备正交拉丁方系的存在。——譯者注

問題是，当 $t$ 不是素数或者素数冪时，問能不能填补 $(t-1)$ 与 $(p^{e}-1)$ 之間的空隙，人們猜想，这将填补不了❶。L. Euler (1782)❷ 猜想了对 $t=6$ 不存在希腊·拉丁方（“36 个軍官的問題”），G. Tarry (1901)❸ 用枚举計算驗証了这个猜想❹。J. Petersen (1901)❺ 用拓扑学所作的証明是錯誤的，而 P. Wernicke (1910)❻的証明❼也由 H. F. MacNeish (1922)❽ 发見了錯誤。但是 MacNeish 用拓扑学所作的証明也有错誤，这已为 F. W. Levi (1942)❾指出。到現在为止，分析的証明，代数的証明以及几何的証明都不成功，如果現在的曲面論有所推广，也許可能成功❿。当 $t$ 为素数或者素数冪时，完备正交拉丁方系是由 H. F. MacNeish (1922)❽的論文第一次給出的。

若 $t$ 是素数或者素数冪，則 $PG[2,t]$ 存在。所以模仿 §7 把它的一条直綫 $UV$ 命名为无限远直綫，令通过这条无限远直綫上的一点 $U$ 的綫束中的直綫号碼为行号碼 $x$，通过另一点 $V$ 的綫束中的直綫号碼为列号碼 $y$。通过不在 $UV$ 上的一点 $P(x, y)$ 的直

---

❶ Bruck-Ryser [23] 証明了对 $t=6, 14, 22, \cdots$，不存在 $t-1$ 个正交拉丁方（見 §15），但这不意味着連 2 个也不存在。1959 年，Bose 等人（[20]，[21]，[22]，[43]，[44]）表明了对 $t=2, 6$ 以外的 $t$ 都可以构造 2 个正交拉丁方。1961年，Johnson 等[34]用群論方法对 $t=12$ 又找到了 5 个正交拉丁方。——譯者注

❷ Euler [25]. Euler 更一般地猜想，对 $t=4m+2$，$m=0, 1, \cdots$，不存在希腊·拉丁方。——譯者注

❸ Tarry [60].——譯者注

❹ 在 §7 中我們説对 $t=6$，$PG[2, t]$ 不存在，乃是指 $t-1=5$ 个正交拉丁方不存在，而这不意味着連 2 个也不存在。

❺ Petersen [45]. 力图肯定 Euler 猜想。——譯者注

❻ Wernicke [63]. 力图肯定 Euler 猜想。——譯者注

❼ 高木貞治：数学小景，岩波，1943 継承了这个錯誤。見科学，14(1944)，42～44 上的訂正。

❽ MacNeish [36]. 力图肯定 Euler 猜想。——譯者注

❾ Levi [5].——譯者注

❿ 如脚注❹所述，Euler 猜想已被否定地解決。——譯者注

綫,除 $UP$ 和 $VP$ 以外,共有 $t-1$ 条,按它們通过 $UV$ 上的那些点加以区别,例如通过第 $j$ 个无限远点的綫束直綫中通过 $P$ 的直綫号碼表为 $b^j_{xy}$。直綫的号碼,按綫束而有所区别。固定 $j$,把 $b^j_{xy}$ 放在 $x$ 行 $y$ 列,則这給出一个拉丁方 $(L_j)$,并且綫束号碼不同的 $(L_j)$ 与 $(L_l)$ $(j\neq l)$ 为正交。反之,設有 $k-1$ 个边长 $t$ 的正交拉丁方,其中第 $j$ 个拉丁方的 $x$ 行 $y$ 列的元素表为 $b^j_{xy}$,并若 $t^2$ 个点 $(x, y)$ 滿足下列 (i) ~ (iii),則任意两条直綫至多只公有一点。(i) 固定 $x$ 时点在一直綫上,(ii) 固定 $y$ 时点在一直綫上,(iii) 固定 $j$ 时,$b^j_{xy}$ 相同的点 $(x, y)$ 在同一直綫上。这样可得到 $k+1$ 种形式的直綫。同一形式的直綫不相交,而不同形式的直綫相交。任意一点都結合着每一条 $k+1$ 种形式的直綫 $(EG_2.2)$,以及 $(0, 0)$,$(0,1)$,$(1, 0)$ 不在同一直綫上 $(EG_2.3)$。若 $y_1\neq y_2$,則通过 $(x_1,y_1)$ 并且与直綫 $y=y_2$ 相交的直綫有 $k$ 条,它們是 $x=x_1$ 和

$$b^j_{xy}=b^j_{x_1y_1} \quad (j=1, 2, \cdots, k-1). \tag{14.19}$$

但是点 $(x, y_2)$ 总共有 $t$ 个,所以 $k\leqslant t$。

现在来定义直綫及綫束的記号法,以便构造**标准型**。一种做法是,定义

$$b^j_{x0}=x, \quad b^j_{0y}=y, \quad b^j_{01}=j, \tag{14.20}$$

而其余由行与行、列与列以及字母与字母的置换导出。另一种做法是,如 §6 那样給通过 $U$ 的直綫記号,并对在不通过 $U$ 和 $V$ 的直綫 $OE$ 上与 $U$ 的直綫相交的 $V$ 的直綫記上与 $U$ 的直綫相同的号碼。$OU$ 上的点的形状是 $(0, b)$,此处特别令 $O$ 为 $(0, 0)$,$E$ 为 $(1, 1)$。这就是說,取任意一点 $P$,令 $UP$ 的号碼为 $x$,$VP$ 的号碼为 $y$,然后从 (6.4) 得到标准形式

$$y=T(x, j, b^j_{xy}). \tag{14.21}$$

这时不假定可分解性条件,从 (6.5) 和 (6.6) 推出

$$b_{0y}^{j}=y, \quad b_{xx}^{1}=0, \quad b_{1j}^{j}=0. \qquad (14.22)$$

在指数 $\lambda$ 不一定是 $t$ 的冪的 OA 中，人們对 $t=2$, $d=2$ 的情形作了較多的研究。$N=2^n$ 的情形是簡单的，为 J. Sylvester (1868) ❶在研究有关代数方程的問題中所解决。

对于 $(4\lambda, 4\lambda-1, 2, 2)$，R. E. A. C. Paley (1933) ❷❸ 研究到 $N=200$. 这是他在解决有关多面体的問題中得到的。根据 Paley 的方法，对于 $N\leqslant 200$，只有 $\lambda=23, 29, 39, 43, 46, 47$ 的情形不能构造，但人們仍未知道这些情形是否存在。对于 $t=2$ 的情形，令 $(+1)$ 对应于一个水平，$(-1)$ 对应于另一个水平，并作 $[N, N]$ 型矩陣，若把其中任意两列看做列矢量，其內积为 0，則这个矩陣叫做**正交矩陣**。从这个正交矩陣去掉同符号的一列，便得到 $(4\lambda, 4\lambda-1, 2, 2)$. 这給出依 §2 意义的最优正交設計。若 $N=2$，則

$$C \stackrel{d}{=} \begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix}, \quad D \stackrel{d}{=} \begin{pmatrix} +1 & -1 \\ -1 & -1 \end{pmatrix} \qquad (14.23)$$

以及 $-C$, $-D$ 是正交矩陣。若 $N>2$，則 $N$ 必須是 4 的倍数。因为，令 $a_{ij}$ 表示任意正交矩陣的第 $i$ 行第 $j$ 列的元素，則

$$\sum_{i=0}^{N-1}(a_{i1}+a_{i2})(a_{i1}+a_{i3})=\sum_{i=0}^{N-1}a_{i1}^{2}=N, \qquad (14.24)$$

但是括号內是 0 或 2，所以乘积是 0 或者 4. 当阶 $N_1$ 和 $N_2$ 的正交矩陣 $U_1$ 和 $U_2$ 分别存在时，把 $U_1$ 置于 $U_2$ 的元素 $(+1)$，$-U_1$ 置于 $(-1)$，便得到阶 $N_1N_2$ 的正交矩陣。因此，可先造出簡单的，然后再用上列矩陣 $C$, $D$ 来扩大。

---

❶ Sylvester [59].——譯者注

❷ 在增山 [8] 的注 16 中举出了 R. L. Plackett & J. P. Burman (1946) 的名字，这在历史上是不正确的。当时在东京大学找不到登載 Paley 論文的期刊。

❸ Paley [42]. Plackett-Burman [46] 利用 Paley 的方法，对 $N\leqslant 100$，不包含 $N=92$，具体給出了 $(4\lambda, 4\lambda-1, 2, 2)$.——譯者注

1° 若存在素数 $p$ 使 $N=p+1$, $p\equiv 3 \pmod 4$，则存在边长 $N$ 的正交矩陣 (R. E. Gilman, 1931) ❶。

2° 若存在素数 $p$ 使 $N=2^k(p+1)$, $k\geqslant 2$, 则存在边长 $N$ 的正交矩陣。若 $p=2$, 或者 $p\equiv 3 \pmod 4$，则这归結于1°. $p$ 只須是奇素数卽可❷ (R. E. A. C. Paley, 1933)。

在正交矩陣 $(4\lambda, 4\lambda-1, 2, 2)$ 中，令行号碼对应品种号碼，列号碼对应区組号碼，并取 $(+1)$ 为 $n_{ij}=+1$, $(-1)$ 为 $n_{ij}=0$, 则得到参数

$$v=b=4\lambda-1,\quad k=r=2\lambda,\quad \lambda=\lambda \tag{14.25}$$

的 SBIB. 利用相补法又得到参数

$$v_c=b_c=4\lambda-1,\quad k_c=r_c=2\lambda-1,\quad \lambda_c=\lambda-1 \tag{14.26}$$

的 SBIB. 一般，若

$$N=\lambda t^2,\quad k=(\lambda t^2-1)/(t-1),\quad p=t,\quad d=2 \tag{14.27}$$

的 $k$ 的最大的 OA 存在，则用序貫混杂法的思想可构造参数

$$v_A=\lambda t^2,\ k_A=\lambda t,\quad b_A=t(\lambda t^2-1)/(t-1),$$
$$r_A=(\lambda t^2-1)/(t-1),\quad \lambda_A=(\lambda t-1)/(t-1) \tag{14.28}$$

的 ARBIB. 反之，若具有上列参数的 ARBIB 存在，则 (14.27) 的 OA 存在。(14.28) 无非是在 (1.16) 中改 $n$ 为 $t$ 和改 $[1+(n-1)t]$ 为 $\lambda$ 而得到的。

BIB 与 OA 的关連性引起了利用差集合来构造 OA 的思想。考虑强度 2 的情形。把阶 $t$ 的模 $\mathfrak{M}$ 的元素 $e_0, e_1, \cdots, e_{t-1}$, 允許适当的重复，排成 $m$ 行 $k$ 列，

$$\begin{matrix} d_{11} & d_{12} & \cdots & d_{1k} \\ d_{21} & d_{22} & \cdots & d_{2k} \\ \vdots & \vdots & & \vdots \\ d_{m1} & d_{m2} & \cdots & d_{mk} \end{matrix} \tag{14.29}$$

❶ Gilman [29].——譯者注

❷ 証明可参看増山[8]的注 16. 但是在該书的扩大法中要使 $+1, 0, -1$ 对应于 $C, D, -C$. 对使 $p\equiv 3 \pmod 4$, $N=2^kp(p+1)$ 的素数 $p$ 也存在。

当作上列矩陣中的任意两列的同行元素的差时，若 $m=\lambda t$，亦即 $\mathfrak{M}$ 的元素，包含 0，每出現 $\lambda$ 次，則利用 $\mathfrak{M}$ 的加法表❶，把加法表中以 $d_{ij}$ 为标号的列代入上列矩陣的 $d_{ij}$，然后把上列矩陣往上下方向扩大 $t$ 倍，便得到 $N=\lambda t^2$ 的 OA。証明是簡单的。对 $t^2$ 个对子 $(e_l, e_j)$，从加法表求

$$e_k = e_l - e_j \tag{14.30}$$

的 $e_k$，并把相同的 $e_k$ 併为一組，便得到 $t$ 个組。对于在加法表中以任意的 $e_j$ 和 $e_l$ 为标号的两列 $(j \neq l)$，取以 $e_i$ 为标号的行的元素的差，則不論 $e_i$ 是什么，总有

$$(e_i+e_j)-(e_i+e_l)=e_j-e_l=\text{一定。} \tag{14.31}$$

但是在 $d$ 表中作差时，同一元素每出現 $\lambda$ 次，所以由置换可把列扩大为 $t$ 倍 (R. C. Bose, K. A. Bush, 1952)❷。

当❸ $p$ 为素数时，可以构造 $A_0 \stackrel{\text{d}}{=} (\lambda t^2, \lambda t, t, 2)$，$\lambda \stackrel{\text{d}}{=} p^u$，$t \stackrel{\text{d}}{=} p^v$。把 $GF[p^{u+v}]$ 的元素表为多項式，令 $v-1$ 次以下的元素的系数相等，$v$ 次以上的元素的系数由零元素置换，然后从 $GF[p^{u+v}]$ 的乘法表便可得到 (14.29)。当 $\lambda_1=p^{u-v}>1$ 时，用同样的方法构造 $(\lambda_1 t^2, \lambda_1 t, t, 2)$，并令 $A_1$ 表示各行每重复 $t$ 次后的矩陣，再把 $A_1$ 排于 $A_0$ 的右边，便得到 $(\lambda t^2, \lambda t+\lambda_1 t, t, 2)$。当 $\lambda_2=p^{u-2v}>1$ 时，先构造 $(\lambda_2 t^2, \lambda_2 t, t, 2)$，并令 $A_2$ 表示各行每重复 $t^2$ 次后的矩陣，再把它排于 $A_0A_1$ 的右边，便得到 $(\lambda t^2, \lambda t+\lambda_1 t+\lambda_2 t, t, 2)$，等等。令 $u/v$ 的整数部分为 $c$，則約束数是

$$k=\lambda t+\lambda_2 t+\cdots+\lambda_c t+1.$$

留意排到 $A_c$ 为止的矩陣是把 $\lambda t$ 个强度 1 的 OA 纵迭起来的矩陣，所以把 $t$ 个字母每加 $\lambda t$ 次便得到最后一列 (R. C. Bose, K. A.

---

❶ 这种加法表見例如森口繁一：統計分析，刘璋温譯，p. 68，本丛书。——譯者注

❷ Bose-Bush [19]。——譯者注

❸ 这一段是根据原著者的"补遺"譯出的。——譯者注

Bush, 1952)。

构造以1的原始 $t$ 乘根 $\omega$ 的幂为元素的等距矩陣，并以幂指数代替其元素，便得到上述的差集合，此处設 $t$ 为素数(增山元三郎, 1957)。

所謂[1]**等距矩陣**，乃是指：(i) 任意两列为正交，以及 (ii) 各个元素的"长度"即絕对値相等的矩陣。在校对中著者发覚若 $t$ 是素数，則利用圓分体的整数性质，可以构造 $(2t^2, 2t+1, t, 2)$. 对于使 $e \overset{d}{=} (t^2-1)/8$ 为奇数的素数 $t$，解的确存在，而对于使 $e$ 为偶数的 $t=7$，解也存在，所以对于一般的奇素数，解也許存在。在这些解中包含着从来用試探誤差法得到的 $t=3$ 的情形以及在此以前解的存否还未知道的 $t=5$ 的情形。大概情况，可参看'科学'，**27** (1957)，11 月号。又，因为以1的原始 $t$ 乘根的幂为元素的两个等距矩陣的直积仍是以1的原始 $t$ 乘根的幂为元素的等距矩陣，所以由上述方法可以构造 $N=2^m t^n$ $(2m \leqslant n, 2 \leqslant n)$ 的情形。

把强度2的 OA 的一行写成一張穿孔卡片。一張卡片可以看做指定着 $k$ 个因子 $t$ 个水平中的任一水平，利用这張卡片做試驗，把試驗結果記入指定該处理組合的那張卡片，然后按列把 $N$ 張卡片分类，这样，若二因子以上的交互作用不存在，則可以无偏地把各个主要效应估計出来。但是在这种場合誤差項的自由度为零，所以除誤差方差已知的場合以外，必須把誤差当作**偶然因子**預先包含于 $k$ 个因子之中。若交互作用存在，則在强度2的正交陣列表中不能把主要效应和交互作用分离开来加以估計。例如在表13.2中，若把两个因子 $A_1$ 和 $A_2$ 安排于[1 0]和[0 1]，則它們的交互作用出現于[1 1]和[1 2]，所以不可能把第三和第四个因子安排于

[1] 这一段是根据原著者的"补遺"譯出的。——譯者注

[11] 和 [12] ❶ ❷．对于三因子以上的高阶交互作用不存在但二因子交互作用可能存在的情形，若利用强度3的OA，則不会产生主要效应与二因子交互作用混杂不能分开的情况。下述定理給出一个方法把强度2的OA扩大为强度3的OA．

一般，由 $t$ 个不同字母組成的 $d$ 位数共有 $t^d$ 个。把这些数分为各有 $t$ 个数的 $t^{d-1}$ 組，記作 $S_1, S_2, \cdots, S_{t^{d-1}}$．这时設对各組中的数作 $t$ 个字母的循环置换后仍属于原来的組。設有 $t$ 个字母組成的 $m$ 行 $k$ 列的矩陣 (14.29)，此处 $m=\lambda t^{d-1}$，若对其中的任意 $d$ 列，属于 $S_1, S_2, \cdots, S_{t^{d-1}}$ 的 $d$ 位数每出現 $\lambda$ 次，則可以构造 $(\lambda t^d, k, t, d)$．作 $S_i$，要先作由 $t$ 个字母組成的所有可能的 $d-1$ 位数字。这样总共得到 $t^{d-1}$ 个数字。在这些字母的左边添加 $t$ 个字母中的任意一个字母。对这样得到的 $d$ 位数字作循环置换，則由一个数字产生一个組 $S_i$．現在以 $d_{ij}$ 所属組 $S$ 的 $t$ 个数字来代替 (14.29) 中的 $d_{ij}$，并排在 $d_{ij}$ 的下边，則行数可以扩大为 $N=tm=\lambda t^d$．这是一个 OA，可同 $d=2$ 的場合一样証明。若(14.29)为强度 $d-1$ 的 OA，則扩大后的强度为 $d$，并且在扩大后的表的右边分别添加一个字母，便可扩大为約束数 $k+1$．例如在头 $n$ 行添加 $t$ 个字母中的任意一个字母，第二个 $n$ 行添加与此不同的任意一个字母，第三个 $n$ 行添加与它們都不同的任意一个字母，……(E. Seiden, 1954) ❸。

表 14.2　$t=2, d=3$

| | | | |
|---|---|---|---|
| $S_1$ | 0 | 0 | 0 |
| | 1 | 1 | 1 |
| $S_2$ | 1 | 1 | 0 |
| | 0 | 0 | 1 |
| $S_3$ | 0 | 1 | 0 |
| | 1 | 0 | 1 |
| $S_4$ | 1 | 0 | 0 |
| | 0 | 1 | 1 |

❶ 对于已供实际利用的正交陣列表中，第一个指出哪里安排因子哪里出現交互作用的著作，恐怕是島田正三：推計学入門(电气书院，1956)。后来aa進一步研究的是田口玄一：公差のきめ方(日本規格协会，1956)。

❷ 为了求交互作用，島田正三构造了正交陣列的补助表；田口玄一研究了点綫图法。——譯者注

❸ Seiden [50]．——譯者注

一般，在强度 $d \overset{\mathrm{d}}{=} e+f-1$ 的正交陣列表中，若 $e$ 因子交互作用或者大于 $e$ 的高阶交互作用不存在，則可以无偏地把 $f$ 因子交互作用以及小于 $f$ 的低阶交互作用估計出来❶ (C. R. Rao, 1946)❷。

---

❶ 參看增山 [7]，附录。

❷ Rao [47]. ——譯者注

# 第4章 設計的存在条件

## §15 SBIB 的存在条件

对于§1中的結合关系，我們考慮下列問題。

$I_1$ 各个区組恰好包含 $k$ 个不同品种。

$I_2$ 任意两个区組的公有数为一定，即 $\mu$.

$II_1$ 各个品种恰好出現于 $r$ 个不同区組。

$II_2$ 任意两个品种的相遇数为一定，即 $\lambda$.

III 結合矩陣为**第二类循环矩陣**❶，其形状为

$$\begin{pmatrix} n_1 & n_2 & \cdots & n_v \\ n_2 & n_3 & \cdots & n_1 \\ \vdots & \vdots & & \vdots \\ n_v & n_1 & \cdots & n_{v-1} \end{pmatrix}, \tag{15.1}$$

此处設各元素取1或者0.

現在，把主对角綫上为 $r$，其余为 $\lambda$ 的 $[v, v]$ 型矩陣記为 $\boldsymbol{B}_{r\lambda}$；分別由 $k$ 和 $\mu$ 代替 $r$ 和 $\lambda$ 的記为 $\boldsymbol{B}_{k\mu}$. **第一个問題是**，求 $[v, b]$ 型結合矩陣 $\boldsymbol{A} \overset{\mathrm{d}}{=} (n_{ij})$ 滿足 $I_1$ 和 $I_2$. 亦即求 $\boldsymbol{A}$ 使

$$\boldsymbol{A}'\boldsymbol{A} = \boldsymbol{B}_{k\mu}. \tag{15.2}$$

**第二个問題是**，与第一个問題成对偶，求 $\boldsymbol{A}$ 滿足 $II_1$ 和 $II_2$，亦即求 $\boldsymbol{A}$ 使

$$\boldsymbol{A}\boldsymbol{A}' = \boldsymbol{B}_{r\lambda}. \tag{15.3}$$

若再要求 $I_1$，則得到 SBIB. **第三个問題是**，求 $\boldsymbol{A}$ 滿足 $I_1$, $I_2$, $II_1$ 和 $II_2$，亦即求 $\boldsymbol{A}$ 使

---

❶ 用由上往下每移一行有一个元素移往右边的第一类循环矩陣来討論，也沒有多大的差异。

$$A'A = AA' = B_{k\lambda} \quad (\lambda=\mu,\ r=k). \tag{15.4}$$

特别，若 $v=t^2+t+1$，$k=t+1$，$\lambda=1$，则这相当于求 $PG[2, t]$。**第四个問題**是由条件 I₁，I₂ 和 III 来决定 $A$，这等于求差集合

$$d_1, d_2, \cdots, d_k, \tag{15.5}$$

而且

$$d_i - d_j \equiv n \pmod v \tag{15.6}$$

对满足 $n \not\equiv 0 \pmod v$ 的任意 $n$，不依赖于 $i$ 和 $j$ 具有一定个数 $\lambda$ 的解。在这些問題中，我們可以証明从第一个到第三个問題是等价的，但第四个問題与它們不等价。例如

$$v=b=55, \quad k=r=27, \quad \lambda=13 \tag{15.7}$$

可由正交矩陣得到，但这不满足下述差集合存在的必要条件。

我們只考虑(11.5)中 $\rho=1$ 的情形。这时，若差集合存在，則有

$$\lambda = k(k-1)/(v-1). \tag{15.8}$$

由于 $v>k$，所以 $k>\lambda$。令 $\lambda$ 为整数，$v$ 和 $k$ 为满足(15.8)以及

$$v>k>\lambda>0 \tag{15.9}$$

的整数。設 $v$ 的素因数 $p$ 依模 4 同余于 3。若 $k-\lambda$ 的平方因数以外部分的約数 $q$ 为奇素数，并且满足整数論中的 **Legendre 符号**[1]

$$\left(\frac{-p}{q}\right) = -1, \tag{15.10}$$

則不能构造 $k$ 个整数依模 $v$ 的差集合 (S. Chowla, H. J. Ryser, 1950)[2]。

証明是簡单的。假設差集合存在，又設

$$S \overset{\mathrm{d}}{=} \sum_{j=1}^{k} \omega^{d_j}, \quad \omega \overset{\mathrm{d}}{=} e^{2\pi i/p}, \tag{15.11}$$

---

[1] 以 $n$ 为模的剩余类中若 $m$ 是某个元素的二次剩余，則定义 $(m/n)=+1$，否則定义 $(m/n)=-1$。

[2] Chowla-Ryser [24]。——譯者注

則由循环矩陣的性质，利用依 $S$ 的复数意义的共轭复数 $\bar{S}$ 得到

$$S\bar{S}=k+\lambda(\omega+\omega^2+\cdots+\omega^{v-1})=k-\lambda. \qquad (15.12)$$

另一方面，考虑对有理数域 $\mathfrak{R}$ 加上 1 的原始 $p$ 乘根 $\omega$ 而得到的圓分体[1] $\mathfrak{R}(\omega)$，并記 $\theta$ 为使 $S$ 中的 $\omega$ 变为其整数幂 $\omega^r$ 的变换，则 $\theta S$ 是 $S$ 在 $\mathfrak{R}(\omega)$ 中的共轭元素。設

$$t \overset{d}{=} S\cdot\theta^2 S\cdot\theta^4 S\cdots\theta^{p-3}S, \qquad (15.13)$$

則 $S$ 在 $\mathfrak{R}(\omega)$ 中的代数范数可定义为 $S$ 的所有共轭元素的乘积，

$$N(S)=t\cdot\theta t, \qquad (15.14)$$

此处 $t$ 和 $\theta t$ 是 $\mathfrak{R}(\omega)$ 中的二次子域 $\mathfrak{R}(\sqrt{(-1)^{(p-1)/2}p})$ 的共轭元素。因此，从关于 $p$ 的条件得到

$$N(S)=[x^2-(-1)^{(p-1)/2}py^2]/4=(x^2+py^2)/4, \qquad (15.15)$$

此处 $x, y$ 是整数。由(15.12)，

$$N(S)=(k-\lambda)^{(p-1)/2}. \qquad (15.16)$$

故

$$x^2+py^2-4(k-\lambda)^{(p-1)/2}=0. \qquad (15.17)$$

这里令 $t$ 为与 $q$ 互素，并不包含平方因数，則可把上式改写成

$$x^2+py^2-qtz^2=0, \qquad (15.18)$$

此处 $x, y$ 和 $z$ 沒有公共的素因数。因为 $q$ 不是 $p$ 的約数，所以

$$(y^{-1}x)^2\equiv -p \pmod q. \qquad (15.19)$$

这与假設矛盾。

現在討論 SBIB 的存在条件。最簡单的是下列情形。

$$|\boldsymbol{B}_{k\mu}|=|\boldsymbol{A}'||\boldsymbol{A}|=|\boldsymbol{A}|^2$$
$$=(k-\lambda)^{v-1}[k+(v-1)\lambda]=k^2(k-\lambda)^{v-1}, \qquad (15.20)$$

[1] G. Fueter: Synthetische Zahlentheorie (Walter de Gruyter, Berlin, 1925)，第8章，或者老些的有 P. Bachmann: Die Lehre von der Kreistheilung (Teubner, 1872).

所以当 $v$ 为偶数时，若 $k-\lambda$ 不是平方数，则 SBIB 不可能存在❶。

在討論其他判定法之前，先証明上列头三个問題是等价的。从第一个問題出发。設

$$k_l \overset{d}{=} n_{1l}+n_{2l}+\cdots+n_{vl}, \tag{15.21}$$

则

$$\sum_{l=1}^{v} k_l n_{il}=\sum_{j=1}^{v}\sum_{l=1}^{v} n_{il}n_{jl}=\lambda(v-1)+r\overset{d}{=}\tau. \tag{15.22}$$

又有

$$\sum_{l=1}^{v} k_l=rv. \tag{15.23}$$

若把上列各式看为关于 $k_1, k_2, \cdots, k_v$ 的联立方程，则我們总可找到不全为 0 的 $k_1, k_2, \cdots, k_v$ 和 $(-1)$，所以

$$D\overset{d}{=}\begin{pmatrix} n_{11} & n_{12} & \cdots & n_{1v} & 1 \\ n_{21} & n_{22} & \cdots & n_{2v} & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ n_{v1} & n_{v2} & \cdots & n_{vv} & 1 \\ 1 & 1 & \cdots & 1 & rv/\tau \end{pmatrix}=\left(\begin{array}{ccc|c} & A & & \begin{matrix}1\\ \vdots \\ 1\end{matrix} \\ \hline 1 & \cdots & 1 & rv/\tau \end{array}\right) \tag{15.24}$$

的行列式等于 0。因此，

$$DD'=\left(\begin{array}{ccc|c} & B_{r+1,\lambda+1} & & \begin{matrix}\rho\\ \vdots \\ \rho\end{matrix} \\ \hline \rho & \cdots & \rho & \sigma \end{array}\right) \tag{15.25}$$

的行列式也等于 0，此处

$$\rho\overset{d}{=}r+rv/\tau, \quad \sigma\overset{d}{=}v+r^2v^2/\tau^2. \tag{15.26}$$

在(15.25)中从上面各行减去倒数第二行，求其行列式，则可把 $v-1$

---

❶ 这个存在的必要条件是由 Chowla-Ryser [24] 和 Shrikhande [51] 独立地得到的。——譯者注

个因数$(r-\lambda)$提出来。再乘$-\rho/\sigma$于最后一行，并把它加上倒数第二行，便得到

$$(r-\lambda)^{v-1}[r-\lambda+v(\lambda+1-\rho^2/\sigma)]=0. \qquad (15.27)$$

由于$r>\lambda$，所以上式第二項等于0．利用(15.26)，便得到

$$(\tau+v)\tau(\tau-r^2)=0. \qquad (15.28)$$

故$\tau=r^2$．因此从$\tau$的定义式(15.22)推出

$$\lambda=r(r-1)/(v-1). \qquad (15.29)$$

其次以

$$\varepsilon^2=-\lambda \qquad (15.30)$$

定义复数$\varepsilon$，并設

$$F\overset{d}{=}\left(\begin{array}{c|c} A & \begin{matrix}\varepsilon\\ \vdots\\ \varepsilon\end{matrix} \\ \hline \varepsilon \quad \cdots \quad \varepsilon & -k \end{array}\right), \qquad (15.31)$$

則有

$$FF'=(r-\lambda)E_{v+1}=F'F, \qquad (15.32)$$

此处$E$是单位矩陣，足碼表示它的阶。从上式去考虑(15.31)，便知

$$A'A=B_{r\lambda}=B_{k\mu}. \qquad (15.33)$$

故$r=k$，$\lambda=\mu$．下面我們只考虑第一个問題。

若

$$v\equiv 3 \pmod 4) \qquad (15.34)$$

以及$k-\lambda$的平方因数以外部分的約数$p$为奇素数，并且

$$\left(\frac{-\lambda}{p}\right)=-1, \qquad (15.35)$$

則第一个問題的解不存在。証明方法与上述差集合的情形相同。

首先根据整数論中的 Lagrange 定理❶❷，任意自然数都可表为四个整数的平方和。因此，存在正整数 $b_1, b_2, b_3, b_4$，使

$$k-\lambda \stackrel{d}{=} b_1^2+b_2^2+b_3^2+b_4^2. \tag{15.36}$$

設

$$\boldsymbol{B}_0 \stackrel{d}{=} \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \\ b_2 & -b_1 & b_4 & -b_3 \\ -b_3 & b_4 & b_1 & -b_2 \\ b_4 & b_3 & -b_2 & -b_1 \end{pmatrix}, \tag{15.37}$$

則

$$\boldsymbol{B}_0\boldsymbol{B}_0' = (k-\lambda)\boldsymbol{E}_4. \tag{15.38}$$

由假定有 $v+1 \equiv 0 \pmod 4$，所以若作这样一个矩陣 $\boldsymbol{B}$：沿着主对角綫排 $(v+1)/4$ 个 $\boldsymbol{B}_0$，其余元素全排 0，則

$$\boldsymbol{B}\boldsymbol{B}' = (k-\lambda)\boldsymbol{E}_{v+1}. \tag{15.39}$$

我們有

$$\boldsymbol{G} \stackrel{d}{=} \left(\begin{array}{c|ccc} k-\lambda & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \boldsymbol{B}_{k\lambda} & \\ 0 & & & \end{array}\right) = (k-\lambda)\boldsymbol{E}_{v+1} + \lambda \left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 0 & 1 & \cdots & 1 \end{array}\right)$$

$$= \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \boldsymbol{A} & \\ 0 & & & \end{array}\right) \left(\begin{array}{c|ccc} k-\lambda & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \boldsymbol{E}_v & \\ 0 & & & \end{array}\right) \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \boldsymbol{A}' & \\ 0 & & & \end{array}\right). \tag{15.40}$$

❶ 高木貞治：初等整数論(共立出版，1925)，86 頁。G. H. Hardy and E. M. Wright: An Introduction to the Theory of Numbers (Oxford Clarendon, 1954), §20.5.

❷ 华罗庚：数論导引(科学出版社，1957)，224 頁。——譯者注

現在設

$$\boldsymbol{x} \overset{\mathrm{d}}{=} (x_0, x_1, \cdots, x_v), \tag{15.41}$$

$$\boldsymbol{x}\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \boldsymbol{A} & \\ 0 & & & \end{array}\right) \overset{\mathrm{d}}{=} \boldsymbol{z} \overset{\mathrm{d}}{=} (z_0, z_1, \cdots, z_v), \tag{15.42}$$

$$\boldsymbol{x}\boldsymbol{B} \overset{\mathrm{d}}{=} \boldsymbol{y} \overset{\mathrm{d}}{=} (y_0, y_1, \cdots, y_v), \tag{15.43}$$

则

$$\begin{aligned} \boldsymbol{x}\boldsymbol{G}\boldsymbol{x}' &= \boldsymbol{x}(k-\lambda)\boldsymbol{E}_{v+1}\boldsymbol{x}' + \lambda\left(\sum_{i=1}^{v} x_i\right)^2 \\ &= (\boldsymbol{x}\boldsymbol{B})(\boldsymbol{x}\boldsymbol{B})' + \lambda\left(\sum_{i=1}^{v} x_i\right)^2 \\ &= \sum_{j=0}^{v} y_j^2 + \lambda\left(\sum_{i=0}^{v} c_i y_i\right)^2 \\ &= (k-\lambda) z_0^2 + \sum_{i=1}^{v} z_i^2. \end{aligned} \tag{15.44}$$

此处我們利用了这样的事实:对适当的有理数 $c_i$,

$$\sum_{i=1}^{v} x_i = \sum_{i=0}^{v} c_i y_i. \tag{15.45}$$

設

$$\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \boldsymbol{A} & \\ 0 & & & \end{array}\right)^{-1} \boldsymbol{B} \overset{\mathrm{d}}{=} \begin{pmatrix} c_{00} & c_{01} & \cdots & c_{0v} \\ c_{10} & c_{11} & \cdots & c_{1v} \\ \vdots & \vdots & & \vdots \\ c_{v0} & c_{v1} & \cdots & c_{vv} \end{pmatrix}, \tag{15.46}$$

则 $c_{ij}$ 是有理数,而且 $(c_{ij})$ 的行列式不为 0. 利用这个 $c_{ij}$ 便可写成

$$y_j = \sum_{i=0}^{v} z_i c_{ij}. \tag{15.47}$$

由于本来对 $\boldsymbol{x}$ 不加上任何約束,所以 $z$ 可以任意选擇。首先令 $z_j$ 取 $+1$ 或者 $-1$,往求 $z_j$ 作为齐次联立方程

$$\varepsilon_j z_j = \sum_{i=0}^{v} z_i c_{ij} (= y_j) \quad (j=1, 2, \cdots, v) \tag{15.48}$$

的解。定义 ± 使 $z_0 \neq 0$。于是从 (15.44) 最后两式的两边可把 $y_l^2$ 和 $z_l^2 (l=1, 2, \cdots, v)$ 消去。假設可适当地选 $\varepsilon_{m+1}, \varepsilon_{m+2}, \cdots, \varepsilon_v$，使得 (15.48) 中最后的 $v-m$ 个式子的右边不包含 $z_{m+1}, z_{m+2}, \cdots, z_v$。例如把最后 $v-m$ 个式子改写时有

$$z_j = \sum_{i=0}^{m} z_i d_{ij} \quad (j=m+1, \cdots, v). \tag{15.49}$$

于是 (15.48) 中的第 $m$ 个式子，以 (15.49) 代入后可以整理成

$$\varepsilon_m z_m = \sum_{i=0}^{m} z_i c'_{ij}, \tag{15.50}$$

此处定义当 $c'_{mm}=1$ 时 $\varepsilon_m=-1$，当 $c'_{mm}\neq 1$ 时 $\varepsilon_m=+1$。这样一来，上式也具有 (15.49) 的形状，而 $m$ 变成了 $m-1$。于是 (15.48) 可由 (15.49) 中令 $m=0$ 的式子来代替。因此，得到满足 $z_0 \neq 0$ 的 (15.48) 的解。故 Diophantus 方程

$$x^2 + \lambda y^2 = (k-\lambda) z^2 \overset{d}{=} ptz^2 \tag{15.51}$$

有 0 以外的解 $(x, y)$。这时，若 $p$ 不包含平方因数，并与 $t$ 互素，则 $-\lambda$ 为 $p$ 的二次剩余，这是矛盾。

利用相同方法，若

$$v \equiv 1 \pmod 4 \tag{15.52}$$

以及 $k-\lambda$ 的平方因数以外部分的約数 $p$ 为奇素数，并且

$$\left(\frac{\lambda}{p}\right) = -1, \tag{15.53}$$

则第一个問題的解不存在。在这个場合，不是 (15.51) 而可导出

$$x^2 = (k-\lambda) y^2 + \lambda z^2 \tag{15.54}$$

(S. Chowla, H. J. Ryser, 1950) ❶.

另一种叙述形式是：对 $v$ 为奇数情形，若 $p$ 是任意奇素数并且

❶ Chowla-Ryser [24]. ——譯者注

是 $r-\lambda$ 的平方因数以外部分的約数，则 SBIB 存在时，

$$\left(\frac{(-1)^{(v-1)/2}\lambda}{p}\right)=1.$$

若 $\lambda$ 为 $p$ 的倍数，令 $\lambda_1$ 和 $a$ 分别为 $\lambda$ 和 $r-\lambda$ 的因数幷与 $p$ 互素。则 SBIB 存在时，

(i) $$\left(\frac{(-1)^{(v-1)/2}\lambda_1}{p}\right)=1,$$

如果 $\lambda$ 的因数 $p$ 的最高次冪为偶数，以及

(ii) $$\left(\frac{(-1)^{(v-1)/2}\lambda_1 a}{p}\right)=1,$$

如果 $\lambda$ 的因数 $p$ 的最高次冪为奇数。特别，若

$$v\overset{\mathrm{d}}{=}t^2+t+1,\quad k\overset{\mathrm{d}}{=}t+1,\quad \lambda\overset{\mathrm{d}}{=}1, \tag{15.55}$$

则相当于(15.34)的式子是

$$t(t+1)\equiv 2 \pmod 4). \tag{15.56}$$

因此

$$t\equiv 1 \quad \text{或} \quad 2 \pmod 4). \tag{15.57}$$

由此可知，若 $t$ 的平方因数以外部分包含依模 4 同余于 3 的素数 $p$，则一直綫上有 $t+1$ 个点的 $PG[2, t]$ 不存在。因为 $k-\lambda=t$，而且 $-1$ 不是 $p$ 的二次剩余。因此，对 $t=6, 14, 21, \cdots$, $PG[2, t]$ 不存在。

SBIB 存在的必要条件还可从以整数为元素的两个矩陣的同余关系来研究。設有两个矩陣 $\boldsymbol{A}$ 和 $\boldsymbol{B}$，以及第三个矩陣 $\boldsymbol{C}$ 使得

$$\boldsymbol{A}=\boldsymbol{C}'\boldsymbol{B}\boldsymbol{C},\quad |\boldsymbol{C}|\neq 0, \tag{15.58}$$

则称 $\boldsymbol{A}$ **同余于** $\boldsymbol{B}$，記作 $\boldsymbol{A}\sim\boldsymbol{B}$. 設 $\boldsymbol{A}$ 为非奇异的对称矩陣，它的元素为整数，阶为 $n$. 設 $D_r$ 为 $\boldsymbol{A}$ 的主子式，阶为 $r$，并且

$$D_r\neq 0,\quad r=1, 2, \cdots, n. \tag{15.59}$$

令 $p$ 为任意奇素数，定义 **Hasse 符号**为

$$c_p(\boldsymbol{A}) \overset{\mathrm{d}}{=} (-1, -D_n)_p \prod_{j=1}^{n-1} (D_j, -D_{j+1})_p$$

$$= (-1, -1)_p \prod_{j=0}^{n-1} (D_{j+1}, -D_j)_p, \qquad (15.60)$$

此处 $D_0 \overset{\mathrm{d}}{=} 1$, 以及 $(m, n)_p$ 是 **Hilbert 符号**[1], 即对非零的任意整数 $m$, $n$, $r$ 和任意素数 $p$, 定义若

$$mx^2 + ny^2 = 1 \pmod{p^r} \qquad (15.61)$$

有整数解 $(x, y)$, 則 $(m, n)_p = +1$, 否則 $(m, n)_p = -1$. 如无特别声明, 考慮 $p$ 包含 $p = \infty$. 根据 **Minkowski-Hasse 定理**[2], 若 $\boldsymbol{A} \sim \boldsymbol{B}$, 則对所有奇素数 $p$,

$$c_p(\boldsymbol{A}) = c_p(\boldsymbol{B}). \qquad (15.62)$$

于是若 SBIB 存在, 則必須有

$$c_p(\boldsymbol{B}_{r\lambda}) = c_p(\boldsymbol{E}) = +1. \qquad (15.63)$$

从 $\boldsymbol{B}_{r\lambda}$ 中其他列減去最后一列, 然后再从其他行減去最下一行而得到的矩陣記作 $\boldsymbol{Q}$. 于是 $\boldsymbol{B}_{r\lambda} \sim \boldsymbol{Q}$, 所以留意

$$D_j = (k-\lambda)^j (j+1), \quad j = 1, 2, \cdots, v-1, \qquad (15.64)$$

$$D_v = |\boldsymbol{B}_{r\lambda}| = k^2 (k-\lambda)^{v-1}, \qquad (15.65)$$

便可推出[3]

$$c_p(\boldsymbol{Q}) = (k-\lambda, -1)_p^{v(v-1)/2} (k-\lambda, v)_p^{2v-3} = +1. \qquad (15.66)$$

这个方法只对 $v$ 为奇数情形才能成为判定条件。这里特别考慮 (15.55) 的情形。設 $t = 2q$, 若存在素数 $q$ 使

$$q \equiv 3 \pmod 4, \qquad (15.67)$$

則 $PG[2, t]$ 不存在。因为, 这时

$$c_p(\boldsymbol{Q}) = (t, -1)_p^{t(t+1)/2} \qquad (15.68)$$

---

[1] B. W. Jones: The Arithmetic Theory of Quadratic Form (J. Wiley, New York, 1950), §10. H. Hasse: Zahlentheorie (Akad. Verl., Berlin, 1949).

[2] C. C. MacDuffee: The Theory of Matrices (Springer, Berlin, 1933).

[3] 見 Shrikhande [51]. ——譯者注

的右肩乘幂为奇数，以及由于 $q$ 是 $t$ 的平方因数以外部分的約数而有

$$(t, -1)_p = -1 \tag{15.69}$$

(R. H. Bruck, H. J. Ryser, 1949) ❶.

**例** 具参数 $v=b=29$, $r=k=8$, $\lambda=2$ 的 SBIB 不存在。

$$c_p(Q) = (6, -1)_p^{29.14}(6, 29)_p^{56} = (3, 29)_p(2, 29)_p.$$

这里令 $p=3$ 便得

$$c_p(Q) = \left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

## § 16 ARBIB 的存在条件

如 § 1 所述，由于 ARBIB 与 SBIB 有类似之点，可以预料，用类似的方法能得到 ARBIB 的存在条件。ARBIB 的存在条件由 § 15 所述的两种方法都可得到，这里只介紹第二个方法。給結合矩陣 $\boldsymbol{A} \stackrel{\mathrm{d}}{=} (n_{ij})$ 添加 $l$ 行，在左端填补 $\boldsymbol{E}_l$，其余填补 0，即

$$\boldsymbol{A}_1 \stackrel{\mathrm{d}}{=} \left(\begin{array}{c|c} \multicolumn{2}{c}{\boldsymbol{A}} \\ \hline \boldsymbol{E}_l & \boldsymbol{O} \end{array}\right), \tag{16.1}$$

$$\boldsymbol{A}_1\boldsymbol{A}_1' = \left(\begin{array}{c|c} \boldsymbol{B}_{r\lambda} & \boldsymbol{A}_l \\ \hline \boldsymbol{A}_l' & \boldsymbol{E}_l \end{array}\right), \tag{16.2}$$

此处 $\boldsymbol{A}_l$ 是 $\boldsymbol{A}$ 的头 $l$ 列所成的子矩陣。这里設 $\mu_{ij}$ 为区組 $B_i$ 和 $B_j$ 的公有数，又設

$$c_{ij} \stackrel{\mathrm{d}}{=} \begin{cases} k\lambda - r\mu_{ij} & (i \neq j,\ i, j = 1, 2, \cdots, l), \\ (r-k)(r-\lambda) & (i=j). \end{cases} \tag{16.3}$$

于是設 $\boldsymbol{C}_l \stackrel{\mathrm{d}}{=} (c_{ij})$ 便有

$$|\boldsymbol{A}_1\boldsymbol{A}_1'| = kr^{1-l}(r-\lambda)^{v-l-1}|\boldsymbol{C}_l|. \tag{16.4}$$

---

❶ Bruck-Ryser [23]. ——譯者注

特别，在 $A_1$ 中令 $l \stackrel{d}{=} b-v$ 的矩陣記为 $A_2$。

$$P \stackrel{d}{=} \left(\begin{array}{c|c} B_{r\lambda} & O \\ \hline O & C_{b-v}F_{b-v} \end{array}\right). \tag{16.5}$$

設

$$F_{b-v} \stackrel{d}{=} [r(r-\lambda)]^{-1} E_{b-v},$$

则

$$c_p(P) = c_p(A_2 A_2').$$

由此得出下列結果。

1) 若 $n, t$ 为奇数，则对下列任一情形，ARBIB 都不存在：(i) $k$ 不是完全平方，(ii) $k$ 虽是完全平方，但是

$$nt \equiv 1 \pmod 4$$

以及 $n$ 的平方因数以外部分包含依模 4 同余于 3 的素数。

2) 若 $n$ 为奇数，$t$ 为偶数，则对下列任一情形，ARBIB 都不存在：(i) $k^2/v$ 不是完全平方，(ii) $k^2/v$ 虽是完全平方，但是

$$n+t \equiv 1 \pmod 4$$

以及 $n$ 的平方因数以外部分包含依模 4 同余于 3 的素数。

3) 对任意的 $t$，若

$$n \equiv 2 \pmod 4$$

以及 $n$ 的平方因数以外部分包含依模 4 同余于 3 的素数，则 ARBIB 不存在。

上列情形，当特别令 $t=0$ 时，包含

$$v=n^2, \quad k=n, \quad b=n^2+n, \quad r=n+1, \quad \lambda=1$$

的存在条件 (S. S. Shrikhande, 1951) ❶。

**例** 对 $n=3$, $t=2$ 的情形，因为 $k^2/v=5$ 不是完全平方，所以具参数

$$v=45, \quad k=15, \quad b=66, \quad r=22, \quad \lambda=7$$

的 ARBIB 不存在。

---

❶ Shrikhande [53]。——譯者注

另一种叙述形式是：

1′) 对奇数 $v$，当 ARBIB 存在时，(i) 若 $r$ 为奇数，则 $k$ 是完全平方，(ii) 若 $r$ 为偶数，则 $k^2/v$ 是完全平方。

2′) 若在 ARBIB 中，

$$r \equiv 2 \quad 或 \quad 3 \pmod 4$$

则 $v/k$ 的因数中每一依模 4 同余于 3 的素数这个素数具偶数幂出现于 $v/k$ 的素因数分解中 (K. N. Majumdar, 1953) ❶。

連結 SBIB 与 ARBIB 的存在定理。若 $\mathrm{SBIB}_1$：

$$v=b=n^2t+n+1, \quad r=k=nt+1, \quad \lambda=t$$

存在，而 $\mathrm{SBIB}_2$：

$$v=b=n(n^2t+n+1)+1, \quad r=k=n^2t+n+1, \quad \lambda=nt+1$$

不存在，则 ARBIB (1.16) 不存在 (S. S. Shrikhande, 1951) ❷。

---

❶ Majumdar [37]。——譯者注

❷ Shrikhande [53]。——譯者注

# 附 表 1[1]

| No. | $v$ | $k$ | $b$ | $r$ | $\lambda$ | $E$ | 系 | |
|---|---|---|---|---|---|---|---|---|
| 1 | 6 | 2 | 15 | 5 | 1 | 60 | U | |
| 2 | | 3 | 10 | 5 | 2 | 80 | B, D | No. 25; $(1, 2, 3), (1, 3, \infty) \bmod 5$ |
| 3 | | 4 | 15 | 10 | 6 | 90 | U | |
| 4 | | 5 | 6 | 5 | 4 | 96 | U | |
| 5 | 7 | 2 | 21 | 6 | 1 | 58 | U | |
| 6 | | 3 | 7 | 3 | 1 | 78 | D, P | $(0, 1, 3) \bmod 7$; $PG[2, 2]$ |
| 7 | | 4 | 7 | 4 | 2 | 87 | C | No. 6 |
| 8 | | 6 | 7 | 6 | 5 | 97 | U | |
| 9 | 8 | 2 | 28 | 7 | 1 | 57 | U | |
| 10 | | 4 | 14 | 7 | 3 | 86 | D, E | $(\infty, 1, 2, 4), (0, 1, 2, 4) \bmod 7$; $(\infty, 3, 6, 5), (0, 1, 2, 4) \bmod 7$ RBIB; $EG[3, 2]$ |
| 11 | | 7 | 8 | 7 | 6 | 98 | U | |
| 12 | 9 | 2 | 36 | 8 | 1 | 56 | U | |
| 13 | | 3 | 12 | 4 | 1 | 75 | D, E, K | $PC(4)[(1, 6, 7)\ S(4)+R] \bmod 8$; $EG[2, 3]$ |
| 14 | | 4 | 18 | 8 | 3 | 83 | D, d | $(1, 2, 3, 5), (1, 4, 5, 8) \bmod 9$; No. 46 |
| 15 | | 5 | 18 | 10 | 5 | 90 | C | No. 14 |
| 16 | | 6 | 12 | 8 | 5 | 94 | C | No. 13 |
| 17 | | 8 | 9 | 8 | 7 | 98 | U | |
| 18 | 10 | 2 | 45 | 9 | 1 | 55 | U | |
| 19 | | 3 | 30 | 9 | 2 | 74 | D | $(1, 2, 3), (1, 3, 7), (1, 5, \infty) \bmod 9$ $PC(1, 4, 7) \bmod 9$ |
| 20 | | 4 | 15 | 6 | 2 | 83 | B | No. 42 |
| 21 | | 5 | 18 | 9 | 4 | 89 | B, D | No. 46; $(\infty, x^0, x^2, x^4, x^6), (0, x^1, x^3, x^5, x^7)$，設 $x$ 为 $GF[3^2]$ 的原始元素。 |
| 22 | | 6 | 15 | 9 | 5 | 93 | C | No. 20 |

[1] 这个表比 Fisher-Yates[28] 中的相应部分丰富。最近 Rao [48] 系統地研究了 $11 \leqslant r \leqslant 15$ 的表。——譯者注

附表 1 (續)

| No. | $v$ | $k$ | $b$ | $r$ | $\lambda$ | $E$ | 系 | |
|---|---|---|---|---|---|---|---|---|
| 23 | | 9 | 10 | 9 | 8 | 99 | U | |
| 24 | 11 | 2 | 55 | 10 | 1 | 55 | U | |
| 25 | | 5 | 11 | 5 | 2 | 88 | D | (0, 2, 3, 4, 8) mod 11 |
| 26 | | 6 | 11 | 6 | 3 | 92 | C | No. 25 |
| 27 | | 10 | 11 | 10 | 9 | 99 | U | |
| 28 | 12 | 3 | 44 | 11 | 2 | 73 | D | (0, 1, 3), (0, 1, 4), (0, 2, 6), (0, 5, $\infty$) mod 11 |
| 29 | | 4 | 33 | 11 | 3 | 82 | D | (0, 1, 3, 7), (0, 1, 3, 5), ($\infty$, 0, 1, 5) |
| 30 | | 6 | 22 | 11 | 5 | 91 | B, D | No. 53; (0, 1, 4, 5, 9, 3), ($\infty$, 2, 6, 7, 8, 10) mod 11 |
| 31 | 13 | 3 | 26 | 6 | 1 | 72 | D | (0, 2, 8), (1, 5, 4) mod 13 |
| 32 | | 4 | 13 | 4 | 1 | 81 | D, P | (0, 1, 3, 9) mod 13; $PG[2, 3]$ |
| 33 | | 6 | 26 | 12 | 5 | 90 | d | No. 59 |
| 34 | | 9 | 13 | 9 | 6 | 96 | C | No. 32 |
| 35 | 14 | 7 | 26 | 13 | 6 | 92 | B | No. 59 |
| 36 | 15 | 3 | 35 | 7 | 1 | 71 | D, K, P | [(1, 6, 11)$S(1)$] $CT$ {1, 2, 3, 10, 8, 13, 14} {5, 11, 15, 12, 7, 6, 9}; $PG[3, 2]$ |
| 37 | | 5 | 21 | 7 | 2 | † | | |
| 38 | | 7 | 15 | 7 | 3 | 92 | D, P | (0, 1, 2, 4, 5, 8, 10) mod 15; $PG[3,2]$ |
| 39 | | 8 | 15 | 8 | 4 | 94 | C | No. 38 |
| 40 | 16 | 3 | 80 | 15 | 2 | 71 | D | ($0_2$, $1_2$, $2_2$), ($0_2$, $2_2$, $5_2$), ($0_1$, $7_1$, $0_2$), ($1_1$, $6_1$, $0_2$), ($2_1$, $5_1$, $0_2$), ($3_1$, $4_1$, $0_2$), ($1_1$, $7_1$, $0_2$), ($2_1$, $6_1$, $6_2$), ($3_1$, $5_1$, $0_2$), ($0_1$, $0_2$, $4_2$) mod 8 |
| 41 | | 4 | 20 | 5 | 1 | 80 | D, E | $PC(5)[(1, 3, 4, 12)S(5)+E]$ mod 15; $EG[2, 5]$ |
| 42 | | 6 | 16 | 6 | 2 | 89 | D | ($0_0$, $0_1$, $0_2$, $1_0$, $2_3$, $3_0$)字母和足碼的双重循环 |
| 43 | | 6 | 24 | 9 | 3 | 89 | B | No. 57 |
| 44 | | 10 | 16 | 10 | 6 | 96 | C | No. 42 |
| 45 | 19 | 3 | 57 | 9 | 1 | 70 | D | (0, 6, 10), (1, 2, 13), (3, 5, 8) mod 19 |
| 46 | | 9 | 19 | 9 | 4 | 94 | D | (0, 2, 4, 5, 6, 7, 10, 13, 14) mod 19; (0, 3, 4, 5, 6, 8, 10, 15, 16) mod 19 |
| 47 | | 10 | 19 | 10 | 5 | 95 | C | No. 46 |

附表 1 (續)

| No. | $v$ | $k$ | $b$ | $r$ | $\lambda$ | $E$ | 系 | |
|---|---|---|---|---|---|---|---|---|
| 48 | 21 | 3 | 70 | 10 | 1 | 70 | D, K | [(1, 4, 10), (2, 5, 11), (3, 6, 12), (7, 14, 18), (8, 15, 16), (9, 13, 17), (19, 20, 21)], $CT$ {1, 4, 7, 10, 13, 16, 19} {2, 5, 8, 11, 14, 17, 20} {3, 6, 9, 12, 15, 18, 21}[(1, 6, 11)$CT$], [(2, 4, 12) $CT$], [(3, 5, 10) $CT$] 最后三个每隔二个 |
| 49 | | 5 | 21 | 5 | 1 | 84 | D, P | (1, 4, 5, 10, 12) mod 21; $PG[2, 2^2]$ |
| 50 | | 6 | 28 | 8 | 2 | † | | |
| 51 | | 7 | 30 | 10 | 3 | 90 | B | No. 64 |
| 52 | 22 | 7 | 22 | 7 | 2 | † | | |
| 53 | 23 | 11 | 23 | 11 | 5 | 95 | D | (1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12) mod 23 |
| 54 | 25 | 3 | 100 | 12 | 1 | 69 | D | (01, 41, 13), (10, 33, 12), (32, 21, 02), (11, 24, 20) mod (5, 5) |
| 55 | | 4 | 50 | 8 | 1 | 78 | D | $(0, 1, 4x+1, x+3), (0, 3x+2, 2x+1, 2) \bmod 5$ |
| 56 | | 5 | 30 | 6 | 1 | 83 | D, E | $PC$ (6) [(1, 3, 16, 17, 20) $S$ (6) + $R$] mod 24; $EG[2, 5]$ |
| 57 | | 9 | 25 | 9 | 3 | 93 | | K. N. Bhattacharya (1944). 見 95 頁 |
| 58 | 27 | 9 | 39 | 13 | 4 | 92 | D, E | ($\infty$, 1, 2, 4, 10, 14, 15, 17, 23), (3, 5, 7, 8, 11, 12, 13, 19, 22), (6, 9, 16, 18, 20, 21, 24, 25, 26) mod 26; $EG[2, 3]$ |
| 59 | | 13 | 27 | 13 | 6 | 96 | D | $(1, x^2, x^2+2x, x^2+x+1, 2x^2+2, x^2+x, x^2+2, 2x, 2x+1, x^2+2x+1, 2x^2+x+1, 2x+2, 2x^2+2x+1) \bmod 3$ |
| 60 | 28 | 4 | 63 | 9 | 1 | 78 | D | $(01_1, 02_1, 10_2, 20_2), (01_2, 02_2, 10_3, 20_3), (01_3, 02_3, 10_1, 20_1), (21_1, 12_1, 22_2, 11_2), (21_2, 12_2, 22_3, 11_3), (21_3, 12_3, 22_1, 11_1), (\infty, 00_1, 00_2, 00_3) \bmod (3, 3)$ |
| 61 | | 7 | 36 | 9 | 2 | 89 | B | No. 67 |
| 62 | 29 | 8 | 29 | 8 | 2 | † | | |
| 63 | 31 | 6 | 31 | 6 | 1 | 86 | D, P | (1, 2, 4, 11, 15, 27) mod 31; $PG[2, 5]$ |
| 64 | | 10 | 31 | 10 | 3 | 93 | D | $[(1_1, 1_2, 1_4, 2_1, 2_2, 2_4, 3_1, 3_2, 3_4, 4_7), (1_1, 1_6, 2_2, 2_5, 3_3, 3_4, 4_3, 4_5, 4_6, 5), (1_2, 1_5, 2_3, 2_4, 3_1, 3_6, 4_3, 4_5, 4_6, 6), (1_3, 1_4, 2_1, 2_6, 3_2, 3_5, 4_3, 4_5, 4_6, 7)]$ 只对足碼依模7簡化。$(1_1, 1_2, 1_3, 1_4, 1_5, 1_6, 1_7, 5, 6, 7), (2_1, 2_2, 2_3, 2_4, 2_5, 2_6, 2_7, 5, 6, 7), (3_1, 3_2, 3_2, 3_4, 3_5, 3_6, 3_7, 5, 6, 7)$ |

附表 1 (續)

| No. | $v$ | $k$ | $b$ | $r$ | $\lambda$ | $E$ | 系 | |
|---|---|---|---|---|---|---|---|---|
| 65 | 34 | 12 | 34 | 12 | 4 | † | | |
| 66 | 36 | 8 | 45 | 10 | 2 | † | | |
| 67 | 37 | 9 | 37 | 9 | 2 | 85 | D | (0, 1, 3, 7, 17, 24, 25, 29, 35) mod 37 |
| 68 | 40 | 13 | 40 | 13 | 4 | 95 | D, P | 把 $a$, $c$, $k$, $m$ 加于 No. 68 的各个区組，从 $a$ 到 $m$ 循环; $PG[2, 3]$ |
| 69 | 41 | 5 | 82 | 10 | 1 | 83 | D | (0, 9, 15, 17, 36), (0, 18, 30, 31, 34) mod 41 |
| 70 | 43 | 15 | 43 | 15 | 5 | † | | |
| 71 | 45 | 5 | 99 | 11 | 1 | 82 | D | $[(1_1, 2_1, x_3, (2x)_3, 0_3), ((2x+1)_1, (x+2)_1, (2x+2)_3, (x+1)_3, 0_3)], (0_1, 0_2, 0_3, 0_4, 0_5)$ mod 3 |
| 72 | | 15 | 66 | 22 | 7 | † | | |
| 73 | 46 | 6 | 69 | 9 | 1 | ? | | |
| 74 | | 10 | 46 | 10 | 2 | † | | |
| 75 | 49 | 7 | 56 | 8 | 1 | 87 | D, E | $PC(8)[(1, 2, 5, 11, 31, 36, 38)S(8)+R]$ mod 48; $EG[2, 7]$ |
| 76 | 51 | 6 | 85 | 10 | 1 | ? | | |
| 77 | 53 | 13 | 53 | 13 | 3 | † | | |
| 78 | 57 | 8 | 57 | 8 | 1 | 81 | D, P | (1, 4, 6, 14, 15, 21, 33, 37) mod 57; $PG[2, 7]$ |
| 79 | 63 | 21 | 93 | 31 | 10 | † | | |
| 80 | 64 | 8 | 72 | 9 | 1 | 89 | D, E | $PC(9)[(1, 6, 8, 14, 38, 48, 49, 52)S(9)+R]$ mod 63; $EG[2, 2^3]$ |
| 81 | | 16 | 84 | 21 | 5 | 95 | E | $EG[3, 2^2]$ |
| 82 | 67 | 12 | 67 | 12 | 2 | † | | |
| 83 | 73 | 9 | 73 | 9 | 1 | 90 | D, P | (1, 2, 4, 8, 16, 32, 64, 55, 37) mod 73; $PG[2, 2^3]$ |
| 84 | 77 | 20 | 77 | 20 | 5 | † | | |
| 85 | 81 | 9 | 90 | 10 | 1 | 90 | D, E | $PC(10)[(1, 13, 35, 48, 49, 66, 72, 74, 77)S(10)+R]$ mod 80; $EG[2, 3^2]$ |
| 86 | 91 | 10 | 91 | 10 | 1 | 91 | D, P | (1, 2, 7, 11, 24, 27, 35, 42, 54, 56) mod 91; $PG[2, 3^2]$ |
| 87 | 92 | 14 | 92 | 14 | 2 | † | | |
| 88 | 94 | 31 | 94 | 31 | 10 | † | | |

Bhattacharya 的解❶

(1,2,5,6,11,12,17,20,23) (1,3,5,7,10,12,18,21,24)
(1,2,9,10,15,16,17,21,25) (1,3,9,11,14,16,18,22,23)
(1,2,13,14,7,8,17,22,24) (1,3,13,15,6,8,18,20,25)
(3,4,9,10,7,8,17,20,23) (2,4,9,11,6,8,18,21,24)
(3,4,13,14,11,12,17,21,25) (2,4,13,15,10,12,18,22,23)
(3,4,5,6,15,16,17,22,24) (2,4,5,7,14,16,18,20,25)
(1,4,5,8,10,11,19,22,25) (5,9,13,6,10,14,17,18,19)
(1,4,9,12,14,15,19,20,24) (5,9,13,7,11,15,20,21,22)
(1,4,13,16,6,7,19,21,23) (5,9,13,8,12,16,23,24,25)
(2,3,6,7,9,12,19,22,25) (7,11,15,8,12,16,17,18,19)
(2,3,13,16,10,11,19,20,24) (6,10,14,8,12,16,20,21,22)
(2,3,5,8,14,15,19,21,23) (6,10,14,7,11,15,23,24,25)
(17,18,19,20,21,22,23,24,25)

[注] $S(\theta)$ 表示把 $\theta$, $2\theta$, …加于其前面的初始区組内的数，以便再构造初始区組，但要依模 $v-1$ 簡化。$R$ 表示加一个∞于其余的字母。$PC(\theta)$ 表示把 0, 1, …, $(\theta-1)$ 加于如上得到的所有初始区組全体，就可生成全部区組。$CT$ 表示对附于其右边的区組，按{ }内的順序作循环置换。No. 36 是 §10 的例 1，希讀者进行比較。在本文中号碼从 0 开始，这与本表的号碼相差一个。? 号表示存否不明的設計。

从 §14 的正交矩陣得到的設計，有許多脫漏了。可参看 Plackett-Burman[46]的表。L. D. Calvin: Biometrics, **10** (1954), 61～88 給出了在 (3.2) 中令 $a=1$, $u=3$ 的表，这里不再列出。

❶ Bhattacharya[14]。——譯者注

# 附录 关于阶 $t$ 的 Galois 域 $GF[t]$

根据在 §7 中对平面射影几何坐标集合 $\mathfrak{C}$ 所作的研究，对阶 $t$ 的 Galois 域 $GF[t]$ 的元素 $a, b, \cdots, x, y, \cdots$，有下列十个性质。

1° **加法唯一性** 对任意两个元素 $a$ 和 $b$，唯一确定(在 $\mathfrak{C}$ 中只存在一个)元素 $x$，使 $a+b=x$。

2° **加法可换律** 对任意两个元素 $a$ 和 $b$，$a+b=b+a$。

3° **加法結合律** 对任意三个元素 $a$，$b$ 和 $c$，

$$(a+b)+c=a+(b+c).$$

4° **减法唯一性** 对任意两个元素 $a$ 和 $b$，唯一确定 $x$ 使 $a+x=b$。对任意元素 $a$，使 $a+x=a$ 的 $x$ 叫做**零元素**，記作 0。0 不依赖于 $a$ 的选择。对任意元素 $a$，使 $a+x=0$ 的 $x$ 記作 $-a$。

5° **乘法唯一性** 对任意两个元素 $a$ 和 $b$，唯一确定 $x$ 使 $ab=x$。

6° **乘法可换律** 对任意两个元素 $a$ 和 $b$，$ab=ba$。

7° **乘法結合律** 对任意三个元素 $a$，$b$ 和 $c$，$(ab)c=a(bc)$。

8° **除法唯一性** 对任意非零元素 $a$ 和任意元素 $b$，唯一确定 $x$ 使 $ax=b$。对任意非零元素 $a$，使 $ax=a$ 的 $x$ 叫做**单位元素**，記作 1 或者 $e$。1 不依赖于 $a$ 的选择。对任意非零元素 $a$，使 $ax=1$ 的 $x$ 叫做 $a$ 的**逆元素**，記作 $a^{-1}$。

9° **分配律** 对任意三个元素 $a$，$b$ 和 $c$，成立着左侧分配律 $(a+b)c=ac+bc$ 和右侧分配律 $a(b+c)=ab+ac$。

10° **阶的有限性** 不同元素的个数为有限。

在上列諸性质中，除去 10° 以后的 $\mathfrak{C}$ 是普通的域，除去 8° 和

10° 以后的 $\mathfrak{C}$ 是可换环，除去6°，8° 和10° 以后的 $\mathfrak{C}$ 是普通的环。若只考虑加法这个結合法則，且只假定 1°，2°，3° 和 4°，則 $\mathfrak{C}$ 是一个模。实数的加減乘除显然满足 1°～9°，因而实数全体形成一个域，但对負的实数 $a$，在这个域中不存在 $x$ 使 $x^2=a$。同样，对 $GF[t]$ 中的任意元素 $a$，在 $GF[t]$ 中不一定包含元素 $x$ 使 $x^2=a$。若在 $GF[t]$ 中包含这样的元素，則称 $a$ 为**二次剩余**，否則称为**二次非剩余**。

为了容易看得清楚起見，我們把加法和乘法对应地做了叙述，但是它們不一定是相互独立的。若假定 6°，則只要 9° 中的一个分配律成立卽可。其实，卽使除去 6° 而推广为**斜域**，如本文所述，仍可由条件 10° 推出 6°。又，卽使除去 2° 和 6°，但若假定 9° 中的两側分配律和 8° 的除法唯一性，則仍可以証明 2°。取任意非零元素 $a$，并設 $b$，$c$ 为 $\mathfrak{C}$ 的任意元素，使有

$$\begin{aligned}(a+a)(b+c)&=(a+a)b+(a+a)c=ab+ab+ac+ac\\&=a(b+c)+a(b+c)=ab+ac+ab+ac.\end{aligned}$$

由 4°，把上式右边第一項和第四項去掉，便有

$$ab+ac=a(b+c)=ac+ab=a(c+b).$$

因为 $a\neq 0$，所以由 8° 有

$$b+c=c+b.$$

对于求联立方程的解或两直綫的交点，除法唯一性是必須的，所以要保存这个性质。这样，除去 6° 和 9° 中的一个分配律，可能成为本质上的推广。这相当于这样的推广，卽 V-W 平面不一定与 D 平面一致❶。

如本文所述，$GF[t]$ 当阶 $t$ 为素数或者素数冪时必存在，而对其他的 $t$ 則不存在。若对同构情形不加以区别，則 $GF[t]$的构

❶ 显然这并不意味着 V-W 平面是构造 $PG$ 的最一般的平面。例如在本文定义的 V-W 平面的自然区域中存在着单位元素，但不假定这一点也可以构造 $PG$。

造仅由 $t$ 决定。証明可参看代数学方面的著作❶，这里只介紹便于应用的表現方法。

令 $a$, $b$ 为任意的两个整数，$p$ 为任意的素数。若 $(a-b)$ 为 $p$ 整除，則記作

$$a\equiv b\,(\mathrm{mod}\ p),$$

并称 $a$ 依模 $p$ 同余于 $b$. 对任意的整数 $a$, $b$, $c$, …, 下列性质成立：

(i) **反射律**　$a\equiv a\,(\mathrm{mod}\ p)$,

(ii) **对称律**　若 $a\equiv b\,(\mathrm{mod}\ p)$，則 $b\equiv a\,(\mathrm{mod}\ p)$,

(iii) **傳递律**　若 $a\equiv b(\mathrm{mod}\ p)$, $b\equiv c\,(\mathrm{mod}\ p)$, 則 $a\equiv c\,(\mathrm{mod}\ p)$,

所以，若对依同余式的意义相等的整数不加以区别，則整数全体可以分为 $p$ 类。这叫做**剩余类**。通常取

$$0, 1, 2, \cdots, p-1$$

为各类的代表，它們所属的类分别記作 $C_0$, $C_1$, …, $C_{p-1}$. 定义 $C$ 之間的結合法則为

$$C_a+C_b=C_x \text{ 意味着 } a+b\equiv x\,(\mathrm{mod}\ p),$$

$$C_aC_b=C_y \text{ 意味着 } ab\equiv y\,(\mathrm{mod}\ p),$$

并令 $C_0$ 为零元素，$C_1$ 为单位元素，則在 $C$ 之間成立着 $1^\circ\sim10^\circ$。$p$ 为素数这个条件对 $8^\circ$ 起作用。这可从下例看出：

$$2x\equiv2\ (\mathrm{mod}\ 4)$$

对 $x=1$ 和 $x=3$ 成立，但是

$$1\not\equiv3\ (\mathrm{mod}\ 4).$$

一般地，若 $p$ 不是素数，

$$ax\equiv ay\,(\mathrm{mod}\ p)$$

而且 $a$ 与 $p$ 不互素，則令它們的最大公約数为 $c$。設 $a=a'c$, $p=p'c$,

---

❶ 見例如弥永昌吉·杉浦光夫：代数学，熊全淹譯，本丛书，1962，§24，定理4。——譯者注

则

$$ax-ay=a(x-y)=a'(x-y)c,$$

由于 $a'$ 与 $p'$ 互素，所以 $x-y$ 必为 $p'$ 除尽，因而

$$x\equiv y\,(\mathrm{mod}\ p').$$

若 $p$ 是素数，则 $p$ 除 0 以外与 $1,2,\cdots,p-1$ 互素，所以 8° 成立。因为 $C_a$ 的集合与 $a$ 的集合同构，$C_a$ 与 $a$ 有一一对应关系，而且和对应于和，积对应于积，所以可不考虑 $C_a$ 而考虑 $a$ 本身为 $GF[p]$ 中的元素。这表明了，$0, 1, \cdots, p-1$ 的加法和乘法的运算与普通的算术完全同样进行，当結果为負时加上 $p$ 的倍数，結果大于 $p$ 时以 $p$ 除之取其剩余，这样对有限个元素所做的和以及积的运算形成一个封閉系。这可以說是以 $p$ 为周期的循环算术。这种算术命名为 **Galois 算术**。

当阶 $t$ 为素数 $p$ 的 $n$ 次冪，此处 $n$ 是正整数时，考虑 $x$ 的 $n-1$ 次多項式

$$R_a(x)\overset{d}{=\!=}a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1},$$

此处系数是 0 到 $p-1$ 的整数，并对 $i=0, 1, 2, \cdots, n-1$，設

$$R_a(x)+R_b(x)=R_c(x)$$

的定义为

$$a_i+b_i\equiv c_i\,(\mathrm{mod}\ p).$$

$R_a(x)\ R_b(x)$ 不一定是至多 $n-1$ 次多項式，所以如 $t$ 为素数的情形那样，欲使 $R_a(x)R_b(x)$ 是至多 $n-1$ 次多項式，就需要以 $n$ 次多項式 $P_n(x)$ 除之，然后取其剩余。那末 $P_n(x)$ 的特性是什么？欲使 8° 成立，必要与充分条件是，$P_n(x)$ 不能分解为以 $GF[p]$ 中元素为系数的低次多項式的积。这个要求对应于整数的素数性。这种多項式是 $GF[p]$ 上的不可約多項式，而在試驗設計法的領域中叫做最小函数（参看附表 2）。对于任意素数 $p$ 和任意正整数 $n$，至

少存在一个最小函数 $P_n(x)$，証明可参看其他著作[1]。由此可知，以 $GF[p]$ 的元素为系数的任意次多项式 $F(x)$ 依**双重模** $P_n(x)$ 和 $p$ 同余于以 $GF[p]$ 的元素为系数的 $n-1$ 次多項式 $R(x)$。記

$$F(x)\equiv R(x)\quad[\text{modd}\ p,\ P_n(x)].$$

其实可令系数为 $GF[t]$ 的元素，此处 $t$ 是素数幂，在这个場合，$R(x)$ 全体成为 $GF[t^n]$ 的元素。这叫做 $GF[t^n]$ 的**多項式表現**。附表 2 中的 $t^n=4^2,\ 4^3$ 就是这种例子。

一般，令 $GF[t]$ 中互不相同的非零元素为

$$a_1,\ a_2,\ \cdots,\ a_{t-1},$$

則乘上 $GF[t]$ 中任意的非零元素 $x$ 以后，它們仍然互不相同。因为，若有相同的元素出現，則由 8° 推出，在 $a_1,\ \cdots,\ a_{t-1}$ 中必包含相同元素。因此，$xa_1,\ xa_2,\ \cdots,\ xa_{t-1}$ 与 $a_1,\ a_2,\ \cdots,\ a_{t-1}$ 在順序上也許有所不同，但总的来說是一致的。故

$$xa_1xa_2\cdots xa_{t-1}=a_1a_2\cdots a_{t-1}.$$

利用 6°，然后以非零的 $a_1a_2\cdots a_{t-1}$ 除上式两边，便得到下列的**圓周等分方程**(图 8.1)：

$$x^{t-1}=1.$$

1 是 $GF[t]$ 的单位元素。这叫做 **Fermat 定理**。最小函数是 $x^{t-1}-1$ 的一个因子。

由于 $GF[t]$ 的阶为有限，所以对非零的任意元素 $a$ 作

$$a,\ aa=a^2,\ aaa=a^3,\ \cdots$$

时，对不相同的乘冪 $k,\ l(>k)$ 有

$$a^k=a^l.$$

因此，以 $a^k\neq 0$ 除上式，便得到

$$a^d=1\quad(d>0),$$

[1] Carmichael [2]，增山 [7]，計画篇附录，或本丛书中弥永昌吉·杉浦光夫著《代数学》，熊全淹譯，1962，§ 24。

此处設 $d=l-k$. 由此可知，存在着 $d$ 的最小值使 $a$ 的正整数幂等于 1，所以这叫做 $a$ 的阶❶。阶为 $t-1$ 的元素叫做 $GF[t]$ 的**原始元素**。若 $t$ 是素数幂，则原始元素是令最小函数等于 0 的方程的根，至少必存在一个。令 $W$ 为原始元素，则由定义有 $W^{t-1}=1$，以及

$$W^0=1,\ W^1,\ W^2,\ \cdots,\ W^{t-2}$$

都不相同，所以 $GF[t]$ 中非零元素可以表为原始元素的幂。0 可表为 $W^{\infty}$. 这叫做 $GF[t]$ 的元素的**幂表现**。特别，若取 $x$ 的多项式为 $x^0,\ x^1,\ x^2,\ \cdots,\ x^{t-2}$，并以 $GF[t]$ 的最小函数除之取其剩余，则 $GF[t]$ 的元素的幂表现与同一元素的多项式表现依同余式的意义相等。

$GF[p^n]$的元素中阶为 $p^k-1$ $(1<k<n)$ 的或者为其約数的元素以及零元素的全体記为 $\mathfrak{K}$. 在 $\mathfrak{K}$ 的元素中令 $a$ 是一个阶为 $p^k-1$ 的元素，则

$$a^{p^k-1}=1.$$

以$(p^k-1)$除$(p^n-1)$，令商为 $Q$，剩余为 $R$，则 $0\leqslant R<p^k-1$，且

$$a^{p^n-1}=1=a^{Q(p^k-1)+R}=a^R.$$

由阶的定义，$R=0$. 利用相同的論証，可知 $k$ 是 $n$ 的約数。令 $a,b$ 为 $\mathfrak{K}$ 中任意两个元素，则利用可换律得到

$$(ab)^{p^k}=a^{p^k}b^{p^k}=ab,$$

利用分配律得到

$$(a\pm b)^{p^k}=a^{p^k}\pm b^{p^k}=a\pm b.$$

故 $ab$ 以及 $a\pm b$ 都包含于 $\mathfrak{K}$. 若 $a\neq 0$，则 $GF[p^n]$中存在 $a$ 的逆元素 $c$，使 $ac=1$. 故

$$(ac)^{p^k-1}=a^{p^k-1}c^{p^k-1}=c^{p^k-1}=1.$$

---

❶ 可知对和应用相同的論証，则存在正整数 $p$ 的最小值使 $pa=0$. 这个 $p$ 是域的**特征** 2。§7 中的构形 $7_3$ 对特征 2 的情形成立。

因此，$c$ 也包含于 $\mathfrak{K}$. 这表明了 $\mathfrak{K}$ 是一个 $GF[p^k]$. 特别令 $k=1$, 则

$$d \stackrel{\text{d}}{=} p-1$$

显然是 $p^n-1$ 的約数。設

$$\theta \stackrel{\text{d}}{=} (p^n-1)/(p-1),$$

则 $GF[p^n]$ 的元素中，0 以及使

$$a^d=1$$

的元素 $a$ 的全体形成一个 $GF[p]$. 在这个場合，令 $W$ 为 $GF[p^n]$ 的一个原始元素，則

$$0,\ W^0,\ W^\theta,\ W^{2\theta},\ \cdots,\ W^{(p-2)\theta}$$

成为 $GF[p]$ 的冪表現。这从下式显然看出：

$$(W^{j\theta})^d=(W^{\theta d})^j=(W^{p^n-1})^j=1^j=1,$$

$$j=0,\ 1,\ 2,\ \cdots,\ p-2.$$

令最小函数为上述形状 $R_a(x)$，則

$$x^\theta \equiv (-1)^n a_0 \quad [\text{modd}\ p,\ P_n(x)].$$

下面列举較为普通的試驗用到的最小函数。

对于同一的阶，别的最小函数可能存在，但就 Galois 域而論，这只不过是同构的东西，所以我們选擇了形状尽可能简单的最小函数列出来。

附表 2　最小函数表

| 阶 | | 阶 | |
|---|---|---|---|
| $2^2$ | $x^2+x+1$ | $5^2$ | $x^2+3x+3$ |
| $2^3$ | $x^3+x+1$ | $5^3$ | $x^3+3x+2$ |
| $2^4$ | $x^4+x+1$ | | |
| $2^5$ | $x^5+x^2+1$ | $7^2$ | $x^2+6x+3$ |
| $2^6$ | $x^6+x+1$ | $7^3$ | $x^3+6x+2$ |
| $3^2$ | $x^2+x+2$ | $11^2$ | $x^2+7x+2$ |
| $3^3$ | $x^3+2x+1$ | | |
| $3^4$ | $x^4+x^3+x^2+2x+2$ | $13^2$ | $x^2+12x+12$ |
| $4^2$ | $x^2+x+U$ | ($U$, $V$ 表示 $GF[2^2]$ 中互不相同的元素，但既不是零元素又不是单位元素) | |
| $4^3$ | $x^3+Vx^2+x+U$ | | |

# 参考文献


[1] R. C. Bose: Least Square Aspects of Analysis of Variance (Institute of Statistics, University of North Carolina, 1949).

[2] R. D. Carmichael: Introduction to the Theory of Groups of Finite Order (Ginn, Boston, 1937), (Dover, New York, 1956).

[3] R. A. Fisher: Statistical Methods for Research Workers (Oliver-Boyd, Edinburgh, 1925, 1954).

[4] R. A. Fisher: The Design of Experiments (Oliver-Boyd, Edinburgh, 1935, 1953).

[5] F. W. Levi: Finite Geometrical Systems(University of Calcutta, 1942).

[6] H. B. Mann: Analysis and Design of Experiments (Dover, New York, 1949)(中譯本,科学出版社,即将出版).

[7] 增山元三郎: 工場技术者のための实験計画法の話、推定篇附录; 計画篇附录(日本規格协会, 1955).

[8] 增山元三郎: 实驗計画法(岩波全书,岩波书店,东京, 1956).

[9] G. Pickert: Projektive Ebenen (Springer, Berlin, 1955).

[10] A. Wald: Notes on the Efficient Design of Experimental Investigation (Columbia University, New York, 1946).

[11] F. Yates: The Design and Analysis of Factorial Experiments(Imperial Bureau of Soil Science, Harpenden, 1937).

[12] E. Artin: Geometric Algebra(Interscience, New York, 1957).

[13] Mme M. L. Dubreil-Jacotin, L. Lesieur et R. Croisot: Leçons sur la Théorie des Treillis des Structures Algébriques Ordonnées et des Treillis Géométriques (Gauthier-Villars, Paris, 1953).


[1]是关于本书不討論的分析法的初等而簡洁的讲义，[2]是有限几何学的教本,适于练习，[5]包含到此为止的有限几何学的研究成果,是一本簡明的讲义，[12]和[13]包含現代射影几何学,但在本稿完成后购到，未能參考。[9]的内容相当于§6和§7,是一本难懂的著作，[6]和[10]对固定模型的多因子試驗尤其有詳細的討論,其中[10]是一本独特的讲义，而[6]适于用来作教本。[3]，[4]和[11]是創始人写的經典著作,值得一讀,但不易看懂。

# 譯者补充文献


[14] K. N. Bhattacharya: On a new symmetrical balanced incomplete block design, *Bull. Calcutta Math. Soc.*, **36** (1944), 91～96.

[15] R. C. Bose: On the construction of balanced incomplete block designs, *Ann. Eugenics*, **9** (1939), 353～399.

[16] R. C. Bose: A note on the resolvability of balanced incomplete block designs, *Sankhyā*, **6** (1942), 105～120.

[17] R. C. Bose: Mathematical theory of the symmetrical factorial designs, *Sankhyā*, **8** (1947), 107～166.

[18] R. C. Bose: A note on Fisher's inequality for balanced incomplete block designs, *Ann. Math. Stat.*, **20** (1949), 619～620.

[19] R. C. Bose and K. A. Bush: Orthogonal arrays of strength two and three, *Ann. Math. Stat.*, **23** (1952), 508～524.

[20] R. C. Bose and S. S. Shrikhande: On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order 4t+2, *Proc. Nat. Acad. Sci. U. S. A.*, **45** (1959), 734～737.

[21] R. C. Bose and S. S. Shrikhande: On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler, *Trans. Amer. Math. Soc.*, **95** (1960), 191～209.

[22] R. C. Bose, S. S. Shrikhande and E. T. Parker: Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.*, **12** (1960), 189～203.

[23] R. H. Bruck and H. J. Ryser: The non-existence of certain finite projective planes, *Canad. J. Math.*, **1** (1949), 88～93.

[24] S. Chowla and H. J. Ryser: Combinatorial problems, *Canad. J. Math.*, **2** (1950), 93～99.

[25] L. Euler: Recherches sur une nouvelle espèce de quarrés magiques, *Verhandlingen uitgegeven door het Zeeuwsch Genootschap der Wetenschappente Vlissingen*, **9** (1782), 85～239; 又 *Commentationes Arithmeticae*, Petrograd, **2** (1849), 302～361; *Leonardi Euleri Opera Omnia*, Teubner, Leipzig and Berlin, Ser. I, **7** (1923), 291～392.

[26] R. A. Fisher: The arrangement of field experiments, *J. Ministry of Agriculture*, **33** (1926), 503～513.

[27] R. A. Fisher: An examination of the different possible solutions of a

problem in incomplete blocks, *Ann. Eugenics,* **10** (1940), 52~75.

[28] R. A. Fisher and F. Yates: *Statistical Tables for Biological, Agricultural, and Medical Research,* 5th ed., Oliver & Boyd, London, 1957.

[29] R. E. Gilman: On the Hadamard determinant theorem and orthogonal determinants, *Bull. Amer. Math. Soc.,* **37** (1931), 30~31.

[30] M. Hall: Projective planes, *Trans. Amer. Math. Soc.,* **54** (1943), 229~277.

[31] M. Hall, Jr.: A survey of combinatorial analysis, *Some Aspects of Analysis and Probability,* John Wiley & Sons, New York, 1958, 76~104.

[32] M. Hall, Jr. and W. S. Connor: An embedding theorem for balanced incomplete block designs, *Canad. J. Math.,* **6** (1954), 35~41.

[33] H. Hanani: The existence and construction of balanced incomplete block designs, *Ann. Math. Stat.,* **32** (1961), 361~386.

[34] D. M. Johnson, A. L. Dulmage and N. S. Mendelsohn: Orthomorphisms of group and orthogonal Latin squares I, *Canad. J. Math.,* **13** (1961), 356~392.

[35] 刘璋温：尤拉方陣,数学通报, 1961, 393~395.

[36] H. F. MacNeish: Euler squares, *Ann. Math.,* **23** (1922), 221~227.

[37] K. N. Majumdar: On some theorems in combinatories relating to incomplete block designs, *Ann. Math. Stat.,* **24** (1953), 377~389.

[38] H. B. Mann: On the construction of sets of orthogonal Latin squares, *Ann. Math. Stat.,* **14** (1943), 401~414.

[39] 増山元三郎：直交配列表の历史について,品质管理, **10** (1959), 578~583.

[40] W. F. Mikhail: An inequality for balanced incomplete block designs, *Ann. Math. Stat.,* **31** (1960), 520~522.

[41] V. N. Murty: An inequality for balanced incomplete block designs, *Ann. Math. Stat.,* **32** (1961), 908~909.

[42] R. E. A. C. Paley: On orthogonal matrices, *J. Math. and Phys.,* **12** (1933), 311~320.

[43] E. T. Parker: Construction of some sets of pairwise orthogonal Latin squares, *Amer. Math. Soc. Notices,* **5** (1958), 815.

[44] E. T. Parker: Orthogonal Latin squares, *Proc. Nat. Acad. Sci. U. S. A.,* **45** (1959), 859~862.

[45] J. Petersen: Les 36 officiers, *Annuaire des Mathématiciens,* 1902, 413~427.

[46] R. L. Plackett and J. P. Burman: Design of optimum multifactorial experiments, *Biometrika,* **33** (1946), 305~325.

[47] C. R. Rao: Hypercubes of strength 'd' leading to confounded designs in factorial experiments, *Bull. Calcutta Math. Soc.*, **38** (1946), 67～78.

[48] C. R. Rao: A Study of BIB designs with replications 11 to 15, *Sankhyā, Ser.* A, **23** (1961), 117～127.

[49] P. M. Roy: A note on the resolvability of balanced incomplete block designs, *Calcutta Stat. Assn. Bull.*, **4** (1952), 130～132.

[50] E. Seiden: On the problem of construction of orthogonal arrays, *Ann. Math. Stat.*, **25** (1954), 151～156.

[51] S. S. Shrikhande: The impossibility of certain symmetrical balanced incomplete block designs, *Ann. Math. Stat.*, **21** (1950), 106～111.

[52] S. S. Shrikhande: Designs for two-way elimination of heterogeneity, *Ann. Math. Stat.*, **22** (1951), 235～247.

[53] S. S. Shrikhande: On the non-existence of affine resolvable balanced incomplete block designs, *Sankhyā*, **11** (1951), 185～186.

[54] S. S. Shrikhande: Relations between certain incomplete block designs, *Contributions to Probability and Statistics, Essays in Honor of Harold Hotelling*, Stanford University Press, 1960, 388～395.

[55] S. S. Shrikhande: A note on mutually orthogonal Latin squares, *Sankhyā, Ser.* A, **23** (1961), 115～116.

[56] J. Singer: A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43** (1938), 377～385.

[57] D. A. Sprott: Some series of balanced incomplete block designs, *Sankhyā*, **17** (1956), 185～192.

[58] J. Steiner: Combinatorische Aufgabe, *J. für die reine und angewandte Mathematik*, **45** (1853), 181～182.

[59] J. J. Sylvester: Thoughts on inverse orthogonal matrices, *Phil. Mag.* (4), **34** (1867), 461～475.

[60] G. Tarry: Le problème des 36 officiers, *Compte Rendu de la session, Assoc. Française pour l'Avancement des Sciences*, **1** (1900), 122～123; **2** (1901), 170～203.

[61] O. Veblen and W. H. Bussey: Finite projective geometries, *Trans. Amer. Math. Soc.*, **7** (1906), 241～259.

[62] O. Veblen and J. H. M. Wedderburn: Non-Desarguesian and non-Pascalian geometries, *Trans. Amer. Math. Soc.*, **8** (1907), 379～388.

[63] P. Wernicke: Das Problem der 36 Offiziere, *Jahresbericht der Deutschen Mathematiker-Vereinigung*, **19** (1910), 264～267.

[64] 山本幸一：ラテン方陣について，数学，**12** (1960), 67～79.

[65] F. Yates: Incomplete randomized blocks, *Ann. Eugenics*, **7** (1936), 121～140.

[66] F. Yates: Incomplete Latin squares, *J. Agr. Sci.*, **26** (1936), 301～315.

[67] W. J. Youden: Use of incomplete block replications in estimating tobacco mosaic virus, *Contributions from Boyce Thompson Institute*, **9** (1937), 41～48.